International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 4, July - August 2016 ISSN 2278-6856

Secured Transmission of a Real Time Image and Text using Advanced Encryption Standard for Military Purpose

Prof. Kundankumar Rameshwar Saraf[1], Prof. Kushal Namdeo Mandge[2], Prof. Pratik Dilip Shah[3], Prof. Komal Shivaji Mule[4], Prof. Manishkumar Horilal Patel[5]

[1235]Assistant Professor in Department of Electronics and Telecommunication,

[4]Assistant Professor in Department of Computer Engineering,
Dr. D. Y. Patil School of Engineering affiliated to Savitribai Phule Pune University, Pune
Maharashtra, India

Abstract

Army requires secure method which can transmit and receive images of current location without unwanted third party intrusion attack. This paper proposes the method in which text and image encryption performed at the transmitter side. This encrypted text and image can be sent through any wired or wireless media to the receiver. At the receiver the decryption of text and image can be performed. For both the encryption and decryption Advanced Encryption Standard is used.

Any other available current technology either performs the text encryption and decryption or performs the image encryption and decryption. But this research proposes the technology which can perform the both text as well as image encryption decryption using the single gadget.

For text encryption and decryption 128 bit text inputs are synthesized and simulated using simple C language code.

For image encryption and decryption any form of image input is synthesized and simulated using simple java code.

This research uses the small gadget which comprises of two different platforms. Each platform is used to execute either C language Code or Java Code.

The result obtain from this research is completely intrusion free and very fast.

Keywords— Advanced Encryption Standard, Code Block Chaining, Rijndael.

1. INTRODUCTION

Encryption and decryption of information is widely used to avoid the unwanted intrusion attack in transmission and storage of digital media. This process can be performed by many methods like Data Encryption Standard, Blow-fish Algorithm, Triple DES algorithm etc. But many of these methods are susceptible to various kinds of attacks like Brute Force Attack, attack on reflectively weak keys, differential cryptanalysis attack etc.

Therefore the need of most secure and flexible algorithm arises. The National Institute of Standards and Technology (NIST) started a search of Federal information Processing Standard (FIPS). This standard should be secure, fast and most flexible. This standard should replace Data Encryption standard. Due to the advancement in Data Encryption standard, this new standard is named as Advanced Encryption Standard (AES). NIST selected Rijndael algorithm which can be universally used in Advanced Encryption Standard (AES).

Since January 1997 National Institute of Standards and Technology (NIST) started the efforts towards developing the Advanced Encryption Standard (AES). AES standard uses symmetric key for the encryption. In 1997 NIST tried to succeed DES and for that it made a worldwide public call for finding the new algorithm. NIST initially selects 15 algorithms. After the detail analysis of selected 15 algorithms, they were reduced down to 5 algorithms. The names of these five algorithms are RC6, MARS, Rijndael, Serpent and Twofish. All these algorithms uses iterated block ciphers. All these five algorithms were determined to be qualified as the algorithm for AES.

After the extensive review the comparative results for all five finalists are obtained. These results are shown in the table 1 given below. Finally Rijndael algorithm is chosen to be high speed, efficient, most secure and flexible for AES standard.

The final stage of evaluation also solicited by worldwide public input was based on three characteristics

1) Security - The algorithm should provide following characteristic under security parameter:

(a) Mathematical soundness,

(b) Resistance to known attacks,

(c) Randomness of output and security compared to other algorithms.

2) Cost – Algorithm should provide high encryption speed with required memory and without any licensing agreements. In other words this algorithm should be royalty free available worldwide.

3) Algorithm and implementation characteristics – Along with simplicity the algorithm should be suitable across a wide range of hardware and software systems.

2. PREVIOUS WORK

Data can be stored in many forms. For example, it is used in the form of DBMS, ontology [7], taxonomies, etc. Data that is decisive has to be encrypted because data is backbone of industry.

2.1International Status

Modified AES for image encryption is proposed in [1]. In this paper, author adds a key stream generator (A5/1, W7) to AES. Due to this the encryption performance increases for the images which are characterized by reduced entropy. The detailed results shown in this paper concludes the superiority of modified algorithm.

The enhanced model of Advanced Encryption Standard is proposed in [2]. This model is mainly proposed for possessing the better range of image encryption and good level of security. By adjusting the Shift Row Transformation the modification process can be carried out. After the proper comparison between the original AES encryption algorithm and the modified algorithm, authors found that modified algorithm produces very good encryption results focusing towards the security against statistical attacks.

For the image security purpose the block-based transformation algorithm is proposed in [3]. For this transformation author uses the combination of image transformation and image encryption techniques. This algorithm is used prior to encryption. Purpose of this algorithm is to confuse the relationship between the generated image and the original image. The experimental results in this paper show that this combinational technique gives higher entropy value and lower correlation value. Also it gives the more uniform histogram and increases security of encrypted images as compared to the Blowfish algorithm alone.

The problem related with simultaneous selective encryption and image compression is addressed by [4].In this paper the AES with Cipher Feedback (CFB) mode is used to perform the selective encryption and image compression is performed by JPEG algorithm. In this way selective encryption and compression of images is easily performed without affecting the compression rate and also keeps JPEG bit stream compliance.

Text and image encryption is decryption using advanced encryption standard is performed in [8]. In this DSP processor and code composer studio is used for the text encryption and decryption. For the image encryption and decryption this paper uses Java Application Platform SDK.

The detail description of Text encryption and decryption with the implementation method is given in [9]. It shows the result by using 128 bit key and 128 bit input message size.

National Status

At National level, the work on this topic is still going on.

Table 1: Some evaluation criteria and results for AES finalists [6]

Algorithm	Security		Speed		Memory	
	No attacks have been reported against any of the finalists, and no other properties have been reported that would disqualify any of them.		Enc/Dec	Key	RAM	ROM
Mars		High	Average	Average	Low end	Low end
RC6		Adequate	High end	Average	Average	High end
Rijndeal		Adequate	High end	High end	High end	High end
Serpent		High	Low end	Average	Average	Average
Twofish		High	Average	High end	High end	Average

3. SYSTEM MODEL

This project captures the image data in real time. Makes the encryption of data using particular code word in AES and transmit it through medium. After reception of data same codeword should be given to decrypt the data. Decryption gives the original image transmits from the source. The similar process can be performed to send the any text data from the transmitter to the receiver. This project uses 128 bit AES algorithm is used in which each character or space or number or symbol consists of 8 bit binary code. Hence 128 ÷ 8 = 16 characters or spaces or symbol or number or mixture of all these can be used as an input message or as a password.

In this way using the same gadget at the same time we can transmit the text data as well as image data. At the transmitter side simultaneous encryption of text and image can be performed. At the receiver side only encrypted data can be obtained. This data is further decrypted by using the password or key. Due to the use of similar password during both the encryption and decryption process this algorithm is called symmetric algorithm. The relevant block diagram of procedure is given in figure 1 below.

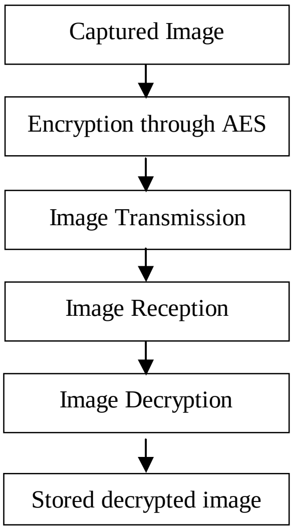


Figure 1 Block diagram of system

4. PROPOSED METHODOLOGY

Different operational modes of AES are Electronic Codebook (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB), Cipher Feedback (CFB) and Counter (CTR).

This research uses the modified version of AES in CBC mode with Public Key Cryptography Standard 5 (PKCS#5) padding. Also for increasing the security salt bytes are appended with the password. In addition to that in this process password based encryption is performed by MD5 and DES algorithm.

In the process of decryption appended salt bytes are removed and decryption is performed using the same password.

Flowchart for image and text encryption and decryption is shown in figure 2 and figure 3 below respectively.

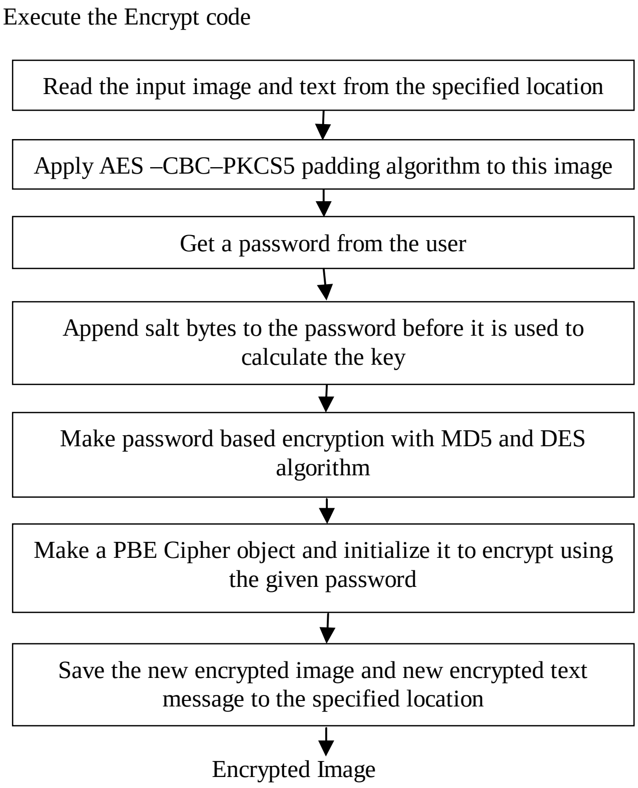

Execute the Encrypt code
Read the input image and text from the specified location
Apply AES –CBC–PKCS5 padding algorithm to this image
Get a password from the user
Append salt bytes to the password before it is used to calculate the key
Make password based encryption with MD5 and DES algorithm
Make a PBE Cipher object and initialize it to encrypt using the given password
Save the new encrypted image and new encrypted text message to the specified location
Encrypted Image

Figure 2 Flowchart of Encryption Process

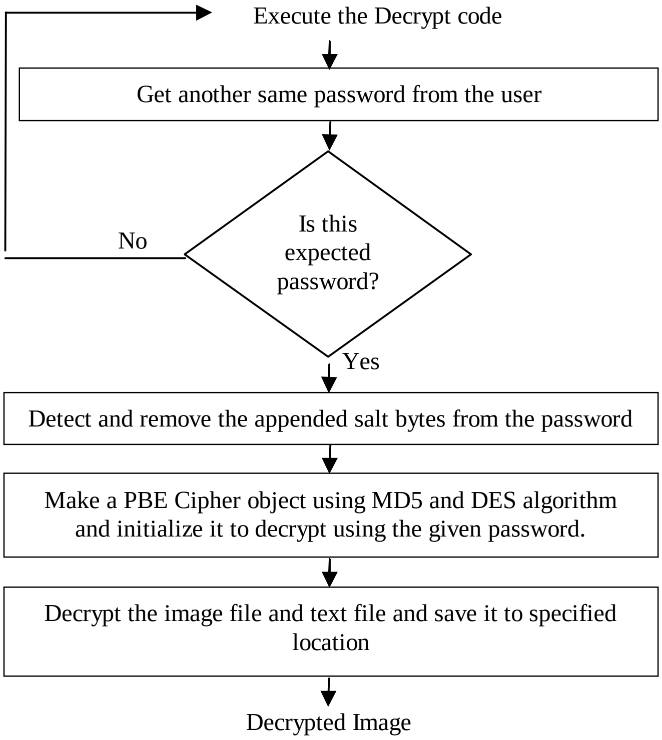

Execute the Decrypt code
Get another same password from the user
Is this expected password?
No
Yes
Detect and remove the appended salt bytes from the password
Make a PBE Cipher object using MD5 and DES algorithm and initialize it to decrypt using the given password.
Decrypt the image file and text file and save it to specified location
Decrypted Image

Figure 3: Flowchart of Decryption Process

Algorithm of the image encryption and decryption

(1) Image of required location is captured by using camera.

(2) This image is stored at desired location in the device.

(3) After pressing encryption key encryption of image using AES starts.

(4) During encryption device asked for the password.

(5) User provides desired password.

(6) After putting password image is encrypted.

(7) User press send key to send this encrypted image to other military colleague.

(8) Receiver press decryption key to decrypt this image.

(9) During decryption device asked for the password.

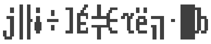
(10) Receiver put the password.

(11) Password used for encryption and decryption should be same for successful decryption.

(12) Decrypted image is observed by the receiver.

5.SIMULATION/EXPERIMENTAL RESULTS

In this research initially user 1 and user 2 decide two different or the similar password for the text and image encryption and decryption. The 128 text input and desired captured image input is provided to the gadget. Using the suitable platform the gadget performs the encryption of this input. The encryption process only completed after inserting the desired password by user 1. In this way two separate encrypted files are generated for text input and image input. The encrypted password protected input is send through transmitter by using internet, Bluetooth, NFC or any other media. At the receiver the encrypted image files and the encrypted text file is observed to user 2. User 2 inserted the already communicated password for the encrypted image and the text file. After inserting the password the original decrypted image and text file can be obtained to the user 2.
The results of text encryption and decryption are as follows.

Input Message: Pqrstuvwxyz
128 bit key or password: ABCDEFGHIJK
Encrypted Message: 
j║i÷]É╪€τë╖·█b

Decrypted Message: Pqrstuvwxyz

In this way we can send any message through this method which has maximum 16 positions including the letters, spaces, symbols and the numbers. The password length should also be maximum 16 positions only.
The results of image encryption and decryption are as follows.

Input image:

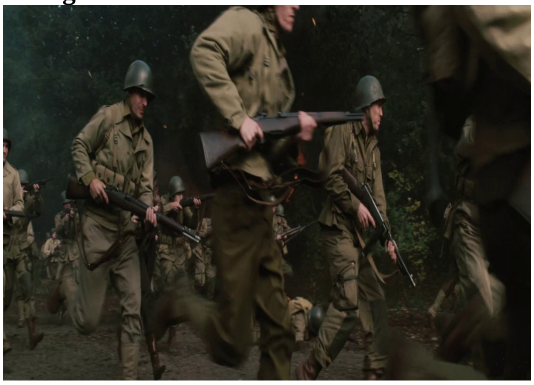


Figure 4: Captured image by the soldier

Key or password: 1234
Encrypted image:

No preview available.

Figure 5: Encrypted image with the help of symmetric password

Decrypted image:

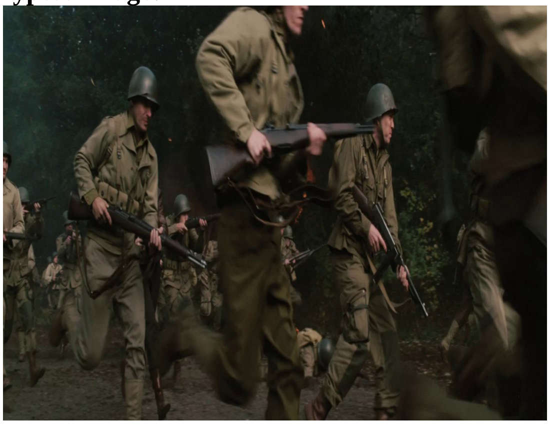


Figure 6: Decrypted image received after inserting the similar password

In this process the image in any format (GIF, JPEG or PNG) can be given to the input of gadget as shown in the figure 4 above. This gadget performs the encryption by using 128 bit password and sends the encrypted image through the transmitter. At the receiver the encrypted image as given in the figure 5 above is obtained. Receiver inserted the similar password to decrypt the image. After decryption the original image is obtained as shown in the figure 6 above.

Encryption and decryption time taken by different images is calculated by Manoj. B, Manjula N Harihar [5]. It is shown in table 2 below.

Average time required by AES for different images is calculated by M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki [1]. It is shown in table 3 below. They also compare encryption time using different algorithms with AES. It is shown in table 4 below. From this table it is found that AES requires least time as compare to other algorithms.

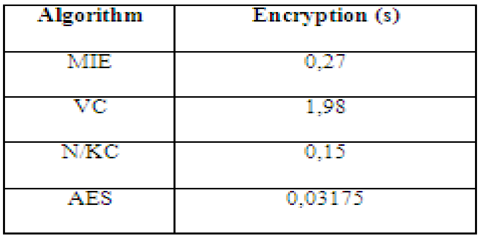
Table 2: Time taken for Different Images [5]

Image Size	Image Size on Disk	Time taken to Encrypt and Decrypt
256*256	66KB	0.707322ms
512*512	258KB	2.796286ms
1024*1024	3.07MB	167.11ms

Table 3: Average Time Required By AES for Different Images [1]

Image (Size)	Image (Size)
Lisaw (256×256)	31.75 ms
Lena(256×256)	31.75 ms
Cheetah(200×320)	29, 25 ms
Clown (200×320)	29, 25 ms
Rose (200×320)	29, 25 ms
Mouse (200×320)	29, 25 ms

Table 4: Encryption Time Using Different Algorithms with Lena as a Test Image [1]



Algorithm	Encryption (s)
MIE	0,27
VC	1,98
N/KC	0,15
AES	0,03175

6.ADVANTAGES OF AES

AES is most useful encryption decryption algorithm because of following advantages [6]

Advantages

- It is royalty free very less cost solution.
- This is most secured completely intrusion free algorithm. Therefore third party intrusion attack is 100% avoided.
- This uses flexible and easy to use method.
- No need of particular training to use this method.
- Simple and symmetric.
- Encrypt and decrypt own files also.
- Fast and uses less computer resources.
- This algorithm prevents the widespread message security compromise.

7.CONCLUSION

The gadget used invented in this research is extremely useful for the soldier. Because soldier can easily capture the image of the terrorist attack and easily send it to the battalion to take the further required actions. Also a text data can send by the soldier. Both text and image data send in the encrypted form and hence unwanted intrusion attack is totally avoided.

8.FUTURE SCOPE

Video encryption and decryption using AES can be developed in future. It will useful for various security agencies to transmit videos through internet.

References

[1] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm For Image Encryption" International Journal of Computer Science and Engineering Volume 1 Number

[2] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, "A New Modified Version of Advanced Encryption Standard(AES) Based Algorithm for Image Encryption", IEEE Transactions on Electronics and Information Engineering, Vol 1,pp.141-145,2010

[3] Mohammad Ali Moh'd Bani Younes, "An Approach To Enhance Image Encryption Using Block-Based Transformation Algorithm", Thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy University of Sains Malaysia, 2009.

[4] W. Puech, J.M. Rodrigues," Analysis and Cryptanalysis of a Selective Encryption Method for JPEG Images" IEEE Transactions on Image Analysis for Multimedia Interactive Services, 2007.

[5] Manoj. B, Manjula N Harihar, "Image Encryption and Decryption using AES" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[6] William Roche, "The Advanced Encryption Standard, The Process, Its Strengths and Weaknesses", University of Colorado, Denver, Spring 2006 Computer Security Class, CSC 7002, Final Paper May 6, 2006.

[7] Komal Mule, "Context based information retrieval based on ontological concepts", 2015 International Conference on Information Processing (ICIP), pages 491 – 495, Dec. 2015.

[8] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), pages 118-126, Volume 3, Issue 3, May – June 2014.

[9] Kundankumar R. Saraf, Sunita P. Ugale, "Implementation of Text Encryption and Decryption in Advanced Encryption Standard", ASM's international e-journal of ongoing research in management and IT, e-ISSN-2320-0065.

AUTHOR

Prof. Kundankumar Rameshwar Saraf received his M.E. degree in VLSI Design and Embedded System from K.arrmveer Kakasaheb Wagh Institute of Engineering Education & Research (K.K. Wagh), Nashik, Savitribai Phule Pune University in 2013. He received his B.E. degree from Shri Shivaji Vidyaprasarak Sanstha's Bapusaheb Shivajirao Deore College of Engineering, Dhule, North Maharashtra University in 2010. He has got 6 years of teaching experience as an Assistant Professor in Electronics and Tele Communication Engineering. He is now performing the research on Light Fidelity Technology and video encryption and decryption using Advanced Encryption Standard.

Prof. Kushal Namdeo Mandge received his M.E. degree in E&TC from Datta Meghe College of Engineering, Airoli, Navi Mumbai, Univeristy of Mumbai in 2014. He received his B.E. degree from SSPM's College of Engineering, Kankavali, University of Mumbai in 2011. He has got 3 years of teaching experience as an Assistant Professor in Electronics and Tele Communication Engineering. He is now performing the research Advanced Encryption Standard, Networking.

Prof. Pratik D. Shah is currently pursuing his Ph. D. from Savitribai Phule Pune University. He completed his post-graduation in VLSI and Embedded from G. H. Raisoni Institute of Engineering and Technology, Pune, Savitribai Phule Pune University in 2013. He has got more than 5 years of teaching experience in graduate level in Electronics and Tele Communication Engineering. His field of research involves Image Steganography, Evolutionary Computation, Data Hiding, Genetic algorithm, Robotics and machine learning.

Prof. Komal Shivaji Mule received M.E in Computer Science from Dr. D. Y. Patil School of Engineering & Technology, Pune, Savitribai Phule Pune University in 2015. She has completed B.E Computer from Marathwada Mitra Mandal's Institute of Technology, Pune, Savitribai Phule Pune University in 2012. Her field of research is information security, data mining, DBMS.

Prof.Manishkumar Horilal Patel received his M.E. degree in E&TC from MITAOE Alandi, Pune, Savitribai Phule Pune University in 2012. He received his B.E Degree from Pravara Rural Engineering College, Loni, Savitribai Phule Pune University in 2009. He has got more than 5 years of teaching experience in graduate level in Electronics and Tele Communication Engineering. His field of research involves Wireless Sensor Network, Antenna Design and Micro strip Patch Antenna.