Arid Zone Journal of Engineering, Technology and Environment. August, 2015; Vol. 11: 50-61

Print ISSN: 1596-2490, Electronic ISSN: 2545-5818
www.azojete.com.ng

IMPLEMENTATION OF IMPROVED AES IMAGE ENCRYPTION IN VB.NET

Mala U. M. B[1]., Ibrahim M. H[2]., Kassim S. O[3]. and Terab M. A[4].

([1]Department of Electrical and Electronic Engineering, University of Maiduguri, Maiduguri, Borno State, Nigeria

[2,3]Department of Electrical and Electronic Engineering Technology, Federal Polytechnic, Damaturu, Yobe State, Nigeria

[4]Department of Computer Engineering, Ramat Polytechnic, Maiduguri, Borno State, Nigeria)

Abstract

Due to the increasing use of images in industrial process, financial institutions, medical and military application, there is every need to achieve secure transmission and storage of digital images. Various methods have been investigated and developed to protect image data for personal privacy and encryption is probably the most obvious solution. This work presents an improvement on the existing Advanced Encryption Standard (AES) Algorithm by implementing it on VB.NET framework. Encryption time of AES was considered to be very long, especially when processing images using encryption key. Therefore, eliminating the use of encryption key will lead to reduced encryption time. Finally, comparisons made of the Improved AES Algorithm with the latest successful Algorithms in image encryption indicates that the Algorithms of Gamil and Pareek encrypts a Kilobyte of image at an average encryption time of 0.7 milliseconds and the average encryption time of the Improved AES is 0.3 milliseconds. This shows that the improvement has been successful.

Keywords*:* Cryptography, image encryption, advanced encryption standard (AES), encryption key, VB.NET

1. Introduction

The security of data to maintain its confidentiality and availability has been a major issue in data communication. For any vital information to be sent, it must have been foremost in the mind of the sender that the information should not get intercepted and read by a rival. Encryption is defined as the conversion of plain message into a form called a cipher text that cannot be read by any person without decrypting the encrypted text. Decryption is the reverse process of encryption; the process of converting the encrypted text into its original plain text, so that it can be read.

The concept of encryption was originally based on the process of manipulating data in form of text for secure storage and transmission over long distances. Encryption techniques are very useful tools to protect secret information. The image encryption is meant to achieve the storage and transmission of image securely over the network. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, data transmission, medical imaging, tele-medicine and military communication etc. The evolution of encryption is moving towards a future of endless possibilities. From the cryptographic point of view, a strong cryptosystem should be secure enough against all kinds of attacks that may try to break the system such as known-plaintext attack, ciphertext-only attack, brute-force attack, statistical attack, and differential attack (Mao *et al.*, 2003). This study is based on the improvement

of an existing and well-known Advanced Encryption Standard (AES) algorithm and implementing it on a different platform of Vb.net for simplicity and additional security. The encryption of both text and images on the same program will be achieved.

Before the modern era, cryptography was concerned solely with the message confidentially (i.e., encryption); conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge; namely the key needed for decryption of that message (OSA, 2010). Encryption was used to (attempt to) ensure secrecy in communications, such as those of spies, military leaders, and diplomats (Becket, 1988). In recent decades, the field has expanded beyond confidentiality concerns to include techniques for massage integrity checking, sender/receiver identity authentication, digital signatures, and interactive proofs and secure computation, among others (David *et al.*, 2009). Rapid developments in digital image processing, medical and military imaging systems and network communications has been witnessed from year 2000 to 2010. The security of digital images/videos has become more and more important. Image encryption is achieved by changing the pixels locations (confusion) or pixels values (diffusion).

One of the public cryptography and widely used in large number of applications such as smart card, cellular phones, automated teller machines, and World Wide Web (www) servers is the AES (Bongeni and Eshghi, 2011). The National Institute of Standard and Technology (NIST) accepted Advance Encryption Standard (AES) that produced by Rijndael in 2001. However, AES suffer from some drawbacks such as, long encryption and decryption time, and patterns appearance in the ciphered image (*Huang et al.*, 2010). The AES algorithm is very difficult to crack and is well suitable to security service applications. It is designed in a way that has better resistance against existing attacks (Sridevi *et al.*, 2006). It has very low memory requirements (Seth and Mishia, 2011), so it is particularly well-suited to embedded applications such as smart cards. The AES algorithm consists of a 128-block length and supports key lengths of 128, 192, and 256 bits. The AES algorithm has three units: encryption, decryption, and key expansion.
The concept of encryption was originally based on the process of manipulating messages in form of text for secure storage and transmission over long distances. Most of the encryption algorithms available were mainly used for text data. Due to large data capacity and real time constrains of image processing, algorithms that are good for textual data may not be suitable for image data. This necessitates for the continuous development of cipher techniques to suit the trend. There are so many image encryption techniques available to be used to protect confidential image data from unauthorized access from which the AES is considered the best, but the issue of processing time and data capacity needs to be addressed (Bhatt and Chandel, 2012). Despite several development efforts by cryptographic experts, the existing AES image encryption algorithms suffer from some drawbacks that include:

i) A high computation as each block is treated using the encryption key.
ii) Extended processing time as a result of the computations.

iii) Appearance of pattern in the ciphered images.
iv) Large hardware and software requirement for the Algorithm to run successfully.

There is the need to look into these drawbacks with the view to finding possible solution through the process of upgrading and improvement.

2. The VB.NET Framework

Vb.net framework, on which the implementation of this improved AES algorithm is proposed, is a software framework developed by Microsoft that includes a large library and provides language interoperability. Each language can use codes written in other languages across several programming languages. The versatility of this framework makes a good advantage for the improved AES Algorithm implementation as it is characterized with high speed, good throughput, less power consumption, less memory requirement and above all, its simplicity.

3. Methodology

3.1. Study Conceptualization

This study is based on the realization of image encryption by improving on the existing Advanced Encryption Standard (AES) Algorithm and implementing it in VB.net framework. The block diagram of the implementation is given in Figure 1.

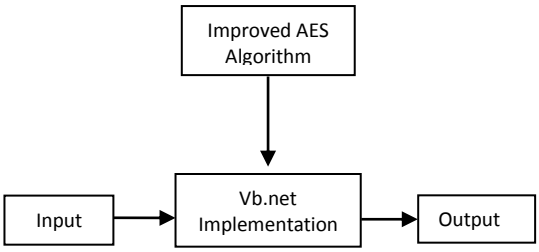


Figure 1: Block diagram of the Improved AES Algorithm implementation

The input to the encryption algorithm is a single 128-bit block of image pixels that is depicted as a square matrix of bytes. The image is first subdivided into pixels, from which a block of4x4 pixels is formed. This block is copied into the State array of 6x6 subdivisions, which is modified at each stage of encryption or decryption. In the encryption process, four (4) different stages are used; one (1) of permutation and three (3) of substitution as given below:

i. Substitute bytes – Uses an S-box to perform a byte-to-byte substitution of the block of image pixels.
ii. Shift rows – A simple permutation. Every row in the state is shifted certain steps to the left. In this operation, each row of the state is cyclically shifted to the left, depending on the row index. The first row is not shifted, the second shifted 1 byte position, the third 2 byte and the fourth 3 byte position.
iii. Mix columns – A substitution that makes use of arithmetic over GF (2^8).

iv. Add round key – A simple bitwise XOR of the current block with the portion of the expanded key.

The output of the encryption is achieved after the final stage of the encryption process from which the state is copied to an output matrix.

3.2 Different Methods for Achieving AES Image Encryption

There are many methods for image encryption. An image will be provided as input and an encrypted image obtained as output. Even then, crackers will attempt different attacks, so it is necessary to increase security. Biometrics such as fingerprints, faces, irises are unique to individuals, so if they are used as keys, the security of the information will be increased. For this, biocryptography is used to increase security of the cryptosystem.

In an attempt to improve the encryption performance in AES-based image encryption, Sridevi *et al.* (2012) advised adding a key stream generator (A5/1, W7) to AES. Images are characterized by reduced entropy. Two forms of key stream generators are used, namely an A5/1 key stream generator and a W7 key stream generator. The A5/1 key stream generator is composed of three linear feedback shift registers (LFSRs): R1, R2, and R3 of length 19, 22, and 23 bits. Each LFSR is shifted, using clock cycles that are determined by the majority function. The author also used the W7 algorithm, which is a symmetric key algorithm supporting key lengths of 128 bits. The W7 cipher has eight similar cells from C1 to C8. Each cell consists of three LFSRs and one majority function. The W7 architecture has a control unit and a function unit. The function unit is responsible for key stream generation. Each cipher cell has two inputs and one output. The one input is the key, and it is the same for all the cells. The other input consists of control signals. Finally, the output is 1 bit long. The output of each cell forms the key stream byte. It offers high security and can be realized easily in both hardware and software.

3.3. The Improved AES Algorithm

AES Algorithm has the best security realization owing to the large substitution and permutation processes involved in the cipher. In this improvement, three modifications are proposed to enhance the performance of AES Algorithm and make it more compatible with ciphering of images and texts alike with reasonable consideration for time of encryption. The modifications are:

(i) The need for a secret key in the encryption process is eliminated and substituted with password. The password here serves the purpose of authorizing the program to run the encryption or decryption process.

(ii) All the stages in the encryption process requiring the processing of encryption key are also eliminated. This drastically reduces the implementation time.

(iii) The type of data to be encrypted (either text or image) will first be identified and redirected properly. The image data will undergo transformation from pixel-to-block and block-to-state. Pixel identity (intensity value and position in row and column) are stored.

Encryption time of AES was considered to be very long, especially when processing images. Therefore, decreasing the number of rounds needed to process the encryption key was proposed and

this will lead to reduced encryption time. The flowchart of the improved AES algorithm is given in Figure 2.

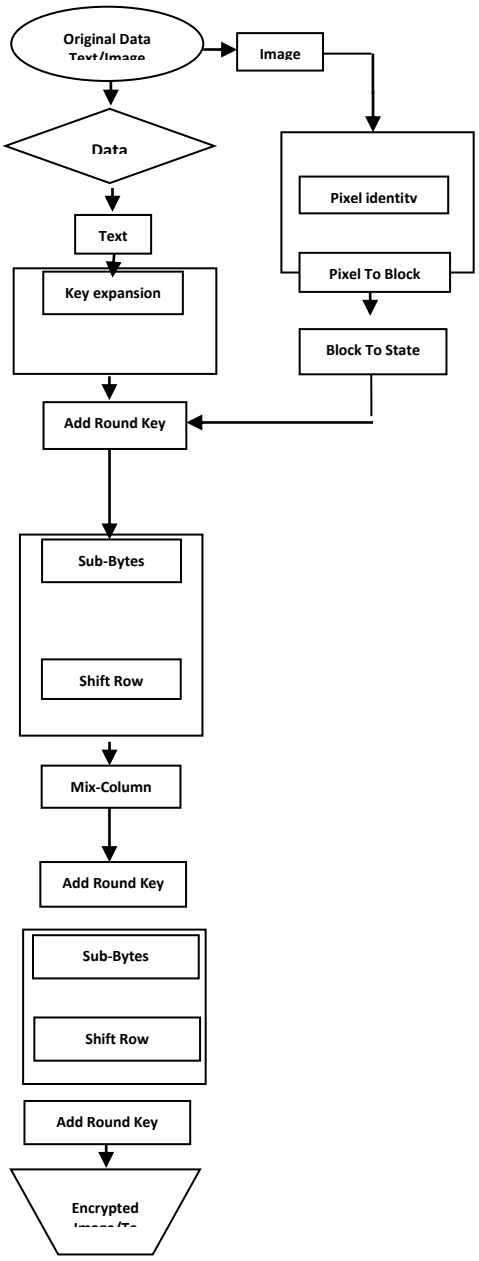


Figure 2: Flowchart of the Improved AES Encryption Algorithm

3.4. Implementation of the Improved AES Algorithm in VB.net Framework

Program for the implementation of Improved AES Algorithm is written in VB.net framework to realize image Encryption and Decryption through the following processes:

i. Image input and Password authorization.
ii. Initial Round

a) The image is identified in pixels and arranged in 4x4 to form a block. The blocks are arranged in 6x6 to form a state on which the next round will apply.

b) The identity of each pixel and block is stored.

iii. Rounds

a) Sub-Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

b) Shift-Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

c) Mix-Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

d) Add-Round-Key

iv. Final Round- Representation with an icon.

4. Results and Discussion

4.1. Encryption Performance of Improved AES

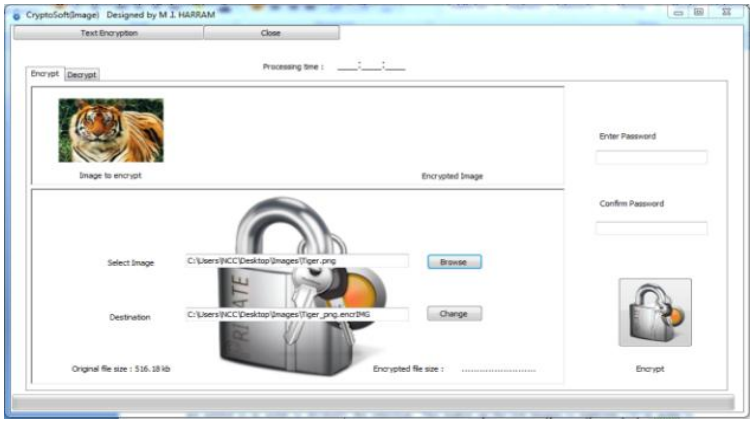
To test our proposed technique that is based on the Improved Advanced Encryption Standard Algorithm, several experiments were performed on the selected images of different formats. The test was to ascertain effectiveness of using the proposed program to achieve secure transmission and storage of images as meaningful information. Six images (Lena, Lady Singer, Hydrangeas in colour, Lena, Cameraman and Pepper in Grey) were encrypted, stored in an external memory and transmitted to an e-mail address via the internet.

The retrieved encrypted images from the external storage device and from the e-mail are decrypted. The test results are presented in Table 1 and are rearranged in order of their sizes. Results of these experiments have proved the efficiency of the Improved AES and its application to digital images.

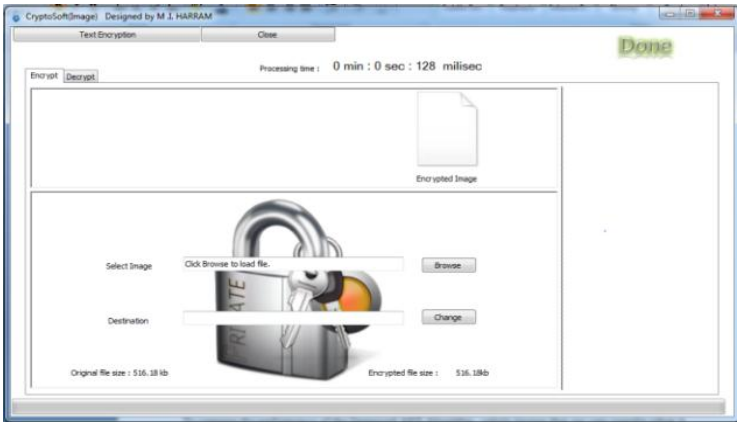
Table 1: Test results of the Improved AES and Original AES on Selected Images

	Stored Encrypted Images		Transmitted Encrypted Images	
IMAGES	SIZE (in KB)	DECREPTION TIME (in milliseconds)	SIZE (in KB)	DECREPTION TIME (in milliseconds)
1. Cameraman	95	124	93	121
2. Lena in Colour	105	132	103	123
3. Lena in Grey	158	143	154	139
4. Pepper in Grey	165	168	160	163
5. Lady Singer	395	261	381	254
6. Hydrangeas	424	314	415	307

Figure 3 (a & b) shows the Graphical User Interface (GUI) of the Improved AES algorithm with image imported before and after encryption.



a



b

Figure 3: The I mproved AES with images (a) and (b) after encryption

4.2. Performance Comparison of Improved AES Algorithm with other Similar Works

To compare the performance of the Improved AES Algorithm, certain images that are very popular when it comes to image encryption are used. These images are mostly in grey or coloured. Six most popular grey images (Baby Duck, Gold Hill, Lena, Pepper, Cameraman and Rose) and the coloured images (Flower, Lady Singer, Play Boy, Lena, Rose and Tiger) are selected to be used.

4.2.1. Pareek et al's Algorithm

Pareek *et al.* (2006) worked on Image Encryption Using Chaotic Logistic Map that achieved image encryption. The approach was based on the use of Chaotic Logistic Map to secure image transfer. The cipher was made robust against attack by modifying the 80 bit secret key after encrypting each

block of 16 pixels of the original image. The colour images of Tiger and Lady Singer were among the test images. Table 2 gives the average ciphering speed of colour images.

Table 2: The average ciphering speed of colour images

S/No.	Image Dimension (in pixels)	Average Encryption Time in Seconds
1.	256 * 256	0.33 – 0.39
2.	512 * 512	0.38 – 0.40
3.	1024 * 1024	6.26 – 6.32
4.	2048 * 2048	25.15 – 25.32

Comparing the Pareek *et al*'sapproach with this proposed Improved Algorithm, the following points are noticeable:

i) The Pareek *et al*'sapproach used the coloured Lady Singer and Tiger as test images. The colour Tiger and Lady Singer images are used as test images in the proposed Improved Algorithm too.

ii) The Improved AES Algorithm encrypts the coloured Lady Singer and Tiger test images in 133 milliseconds and 156 milliseconds respectively, despite the fact that their dimensions are much greater than those whose average encryption time using the Pareek *et al*'s approach was between 330 to 390 milliseconds.

The Encryption times of Pareek *et al's* Algorithm and that of the Improved AES Algorithm on the two test images are presented in Table 3 and the comparison is shown in Figure 4**.**

Table 3: Encryption times of Pareek et al vs Improved AES Algorithms

Images in Kilobytes	Pareek et al's Algorithm in Milliseconds	Improved AES Algorithm in Milliseconds
(1) Lady Singer (456)	330	133
(2) Tiger (556)	390	156

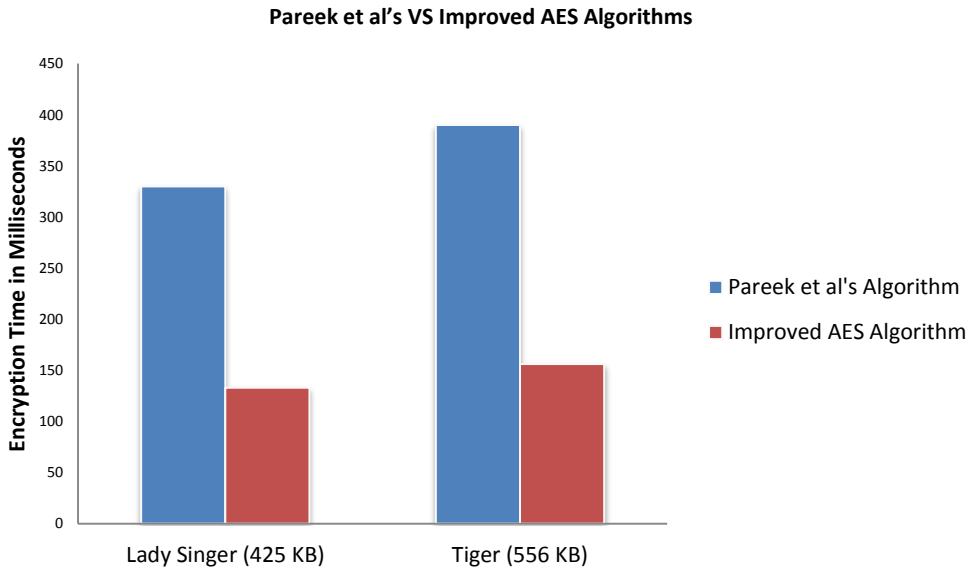


Figure 4: Comparison of Pareek et al's Algorithm and the Improved AES

It can be concluded here that the Improved Algorithm encrypts the same Tiger and Lady Singer colour images of dimension (509*331) and (402*375) in 156 milliseconds and 133 milliseconds respectively. Considering the results in Table 4.3 obtained from the work of Pareek et al, (2006), the test images of Tiger and Lady Singer would have to be encrypted with the average encryption time of 380 to 400 milliseconds, which is almost 200% larger than what is obtained with the Improved AES Algorithm. Hence, the Improved Algorithm is comparatively faster.

4.2.2. Gamil and Sanjay's Algorithm

Equally important, Gamil and Sanjay, (2013) proposed a Bit-Level Encryption and Decryption of Image Using Genetic Algorithm. Their work was aimed at achieving image encryption based on the use of Genetic Algorithm with pseudorandom number generator to encrypt image stream. The main feature of this approach is to achieve high security and high feasibility for easy integration of the encrypted image with digital image transmission application. Many experiments are carried out for defining the competency of the proposed technique. In this part, the proposed technique is applied on the images which have different formats and sizes. The image is Lena coloured with dimension of 135 * 131mm, size 297 KB split in (a) Red, (b) Green and (c) Blue. The encryption/decryption process of each of the RBG split image takes between 76 and 100 milliseconds. The result of the experiment is presented in Table 4.

Table 4: Experimental result of Gamil and Sanjay's Algorithm

Original Image Lena (colored)	Dimension In Pixels	Image Size Before Encryption (KB)	Image Size After Encryption (KB)
(a) Red	259 * 194	140	138.4
(b) Green	2050*1153	145	143.8
(c) Blue	225 * 225	12	12

Comparing the results of the Gamil and Sanjay's technique with this proposed Improved AES Algorithm, the following points are noticeable:

i) The original image used is Lena in colour, 135*131, 297 KB encrypted in about 228 milliseconds. The same Lena colour image is used in the proposed Improved AES Algorithm, but with 472*472, size 557.5 KB, encrypted in 164 milliseconds.
ii) The Lena colour image was split in RBG before encryption, whereas in the Improved Algorithm, the whole image is encrypted at once.

The Encryption rates of the Gamil and Sanjay's Algorithm and the Improved AES Algorithm are calculated and presented in Table 5 and the comparison is presented in Figure 5.

Table 5: Encryption rates of Gamil& Sanjay's VS Improved AES Algorithms

Image Size in Kilobytes	Gamil's Algorithm in Milliseconds	Improved AES in Milliseconds
279	228	82
558	456	164

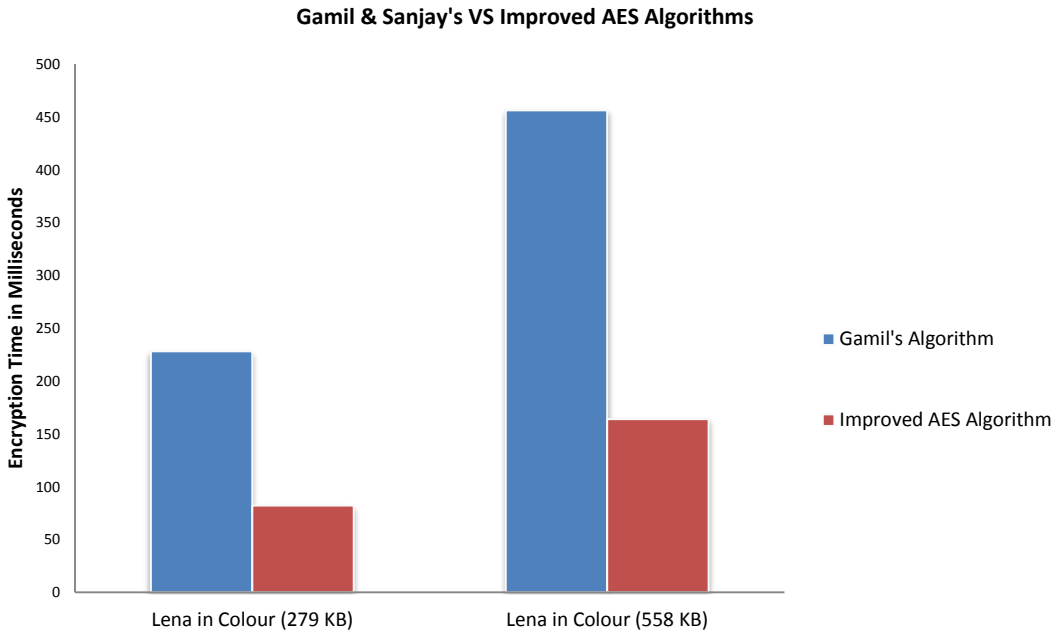


Figure 5: Comparison of Gamil's Algorithm and the Improved AES

It can be concluded here that the Improved Algorithm encrypts the same Lena colour image of twice dimension (472*472 and 135*131) and size (557.5KB and 297KB) in 164 milliseconds against 228 milliseconds. The Improved Algorithm is comparatively faster.

5. Conclusion

This work successfully improves a system for implementing the AES encryption and decryption on the VB.net framework. The original AES algorithm is slow because it is computationally expensive, particularly with image encryption. It is almost impossible to extract the original image encrypted with the proposed improved AES, even if the algorithm is known without the knowledge of the encryption password. In this algorithm, the image is encrypted after a number of rounds, which makes the computation more complex.

The proposed improved AES approach offers enhanced security. It aims to provide user satisfaction by transmitting personal and sensitive image data securely with utmost confidentiality. The Advanced Encryption Standard offers the flexibility of using S-box and strong transformations. Thus the algorithm provides many different flexible implementations. Lastly, the encryption of both text and images on the same program is achieved without necessarily separating the programs independently. This gives an insight into understanding the concepts of image cryptography along with the importance of secure image transmission.

References

Becket, B. 1988. Introduction to Cryptography. Blackwell Scientific Publication, New York.

Bhatt, V. and Chandel, GS. 2012. Implementation of new advanced Image Encryption Algorithm to enhance the security of multimedia component. International Journal of Advanced Technology and Engineering Research, 2 (4): 13-20.

Borujeni, SE. and Eshghi, M. 2011. Chaotic image encryption system using phase magnitude transformation and pixel substitution. Telecommunication System, Springer Science and Business Media. pp.13.

David, A., Li, S., Li, G., Alvarez, AW. and Halang, A. 2009. Cryptanalysis of an Image Encryption scheme based on a new total Shuffling Algorithm. Elsevier Journal of Science, 41 (5): 2613-2616.

Gamil, RS. and Sanjay, NT. 2013. Bit-Level Encryption and Decryption of Images using Genetic Algorithm: A new approach. International Journal of Information Technology, 1(6): 1-5.

Huang, CW., Yen, CL., Chiang, CH., Chang, KH. and Chang, CJ. 2010. The five modes AES applications in sounds and images. 6th International Conference on Information Assurance and Security, IEEE.

Mao, Y., Chen, G. and Lian, S. 2003. A novel fast image encryption scheme based on 3D chaotic Baker maps. International Journal of Bifurcation and Chaos.14: 3613.

Optical Society of America 2010. Long distance, top secret messages: Science Daily.Retrieved from http://www.sciencedaily.com/releases/2010/10/10101917803.htm

Pareek, NK., Patidar, V. and Sud, KK. 2006. Image encryption using chaotic logistic map. Image and Vision Computing, 24: 926–934.

Seth, SM. and Mishra, R. 2011. Comparative analysis of Encryption Algorithms for data communication. International Journal of Computer Science and Telecommunications, 2(2): 292-294.

Sridevi, SSP., KarthigaiKumar, P. Mangai, NMS. and Vanathi, PT. 2012. Survey on efficient, low-power, AES Image Encryption and Bio-cryptography schemes. Smart Computing Review, 2(6): 379-390.