New Advance Encryption Standard to Analyze Encrypted Image Quality

Jaspal Kaur Saini
Department of Computer Science and Engineering
National Institute of Technology
Jalandhar, Punjab, India

Kriti Saini
Department of Information Technology
Green Hills Engineering College
Solan, Himachal Pradesh, India

ABSTRACT
Modern advancement in information technology has enabled pervasive use of multimedia data in variety of applications. Due to increased use of multimedia data on internet it is desired to secure the confidential multimedia data. This paper proposes a new encryption scheme as New Advance Encryption Standard for image encryption. AES is based on substitution- permutation network which is fast for both software and hardware. The New Advance Encryption Standard (NAES) proposes a new encryption scheme by introducing more potential shift row transformation than that of original AES. This NAES allows for more security and better image quality measures. Experimental results are also provided to demonstrate the effectiveness of proposed encryption scheme.

General Terms
Cryptography, Encryption, Decryption, Image Encryption.

Keywords
Advance Encryption Standard (AES), New Advance Encryption Standard (NAES), Image Encryption, Shift Row Transformation, Statistical Analysis.

1. INTRODUCTION
Modern advancements in information technology have enabled pervasive uses of digital multimedia data in a variety of scientific, government, business, and consumer applications. Cryptography provides mechanism for securing and authenticating the transmission of information across insecure channels. Multimedia security involves the protection of digital audio, video and images against illegal access, tampering, piracy, storage, and transmission. Encryption provides the mechanisms to secure the data in various ways.

The art and science of securing message is termed as cryptography[1]. Cryptography can be categorized as: Symmetric Key Cryptography, Asymmetric Key Cryptography[2][3].

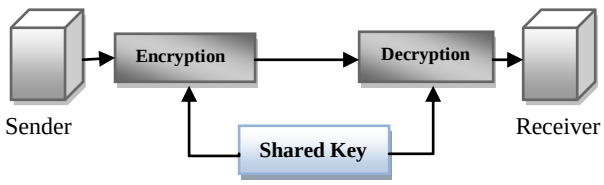

Fig 1: Symmetric Key Cryptography

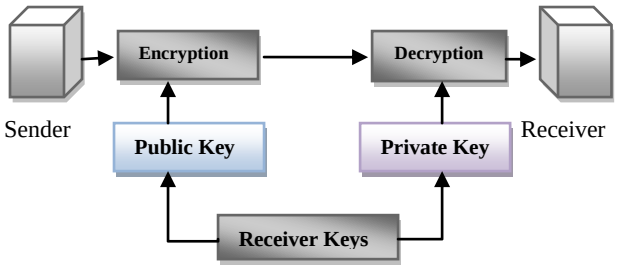

Fig 2: Asymmetric Key Cryptography

2. IMAGE ENCRPTION
An image is an artifactual object. A digital image can be represented as finite set of digital values named pixels or picture elements. To digitize an image two operations are done: Sampling, Quantization[4][5].

Image encryption techniques try to convert original image to cipher image that is hard to understand and to keeps the image confidential between users, i.e. without decryption key no one can access the content. The image contains various different properties: high redundancy and high correlation among adjacent pixels that demands special encryption algorithm for images.

This paper proposes a new encryption scheme as modification of AES algorithm. AES is based on substitution-permutation network which is fast for both software and hardware[6]. The modification is mainly emphasized on both Shift Row Transformations. If the value in first row and first column of state matrix is even then first row remains unchanged; each bytes in second, third and fourth are cyclically shifted left over different numbers, else each bytes in second, third and fourth are cyclically shifted right over different numbers while the first row remains unchanged. This modification allows for more security and better image quality measures.

This paper is organized in following sections: Section 3 gives brief review of AES algorithm. Section 4 explains the proposed encryption scheme for greater security. Experimental results are shown in section 5. Section 6 shows performance evaluation of NAES. The paper is concluded in last section.

3. AES ALGORITHM

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001[7].Based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal which was evaluated by the NIST during the AES selection process[8]. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. AES algorithm is governed by four transformations which are discussed in following subsections.

Table 1. AES Parameters

Key Length	Rounds
128 bit	10
192 bit	12
256 bit	14

3.1 Add Round Key

For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. Add Round Key is an xor between state and the round key. This transformation is its own inverse.

3.2 Sub Byte Transformation

SubByte is a substitution of each byte in the block independent of the position in the state. This is an S-box. This is the non-linear transformation. The S-box used is proved to be optimal with regards to non-linearity. The S-box is based on arithmetic in GF(2^8). The inverse S box can easily be constructed from S box.

3.3 Shift Row Transformation

The Shift Rows step operates on the rows of the state. It cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n is shifted left circular by n-1 bytes. The transformation is clearly invertible by shift in opposite direction by the same amount.

3.4 Mix Column Transformation

Each column in the state is considered polynomial with the byte values as coefficients. The columns are transformed independently by multiplication with special polynomial c(x). c(x) has an inverse d(x), that is used to reverse the multiplication by c(x).

3.5 AES Encryption and Decryption

AES encryption consists of several steps as shown by Fig 3. After an initial round key, round function is applied to data block. This round function consists of the transformations as shown in the Fig 3. The Decryption structure has exactly the same sequence of transformation as in the encryption structure. The inverse of transformations allows the key schedules to be identical for encryption and decryption.

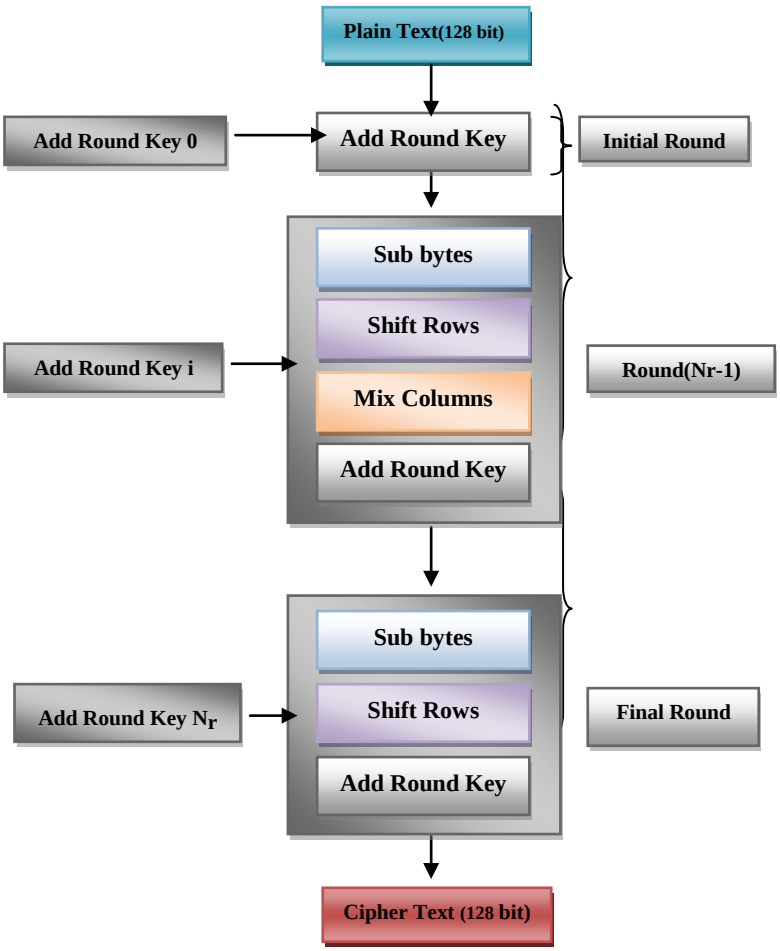

Fig 3: AES Encryption Structure

4. NEW AES ALGORITHM

We presented the new AES algorithm to provide better security by proposing more potential Shift Row transformation. New Shift Row transformation is shown in figure as:

a1	a2	a3	a4
a5	a6	a7	a8
a9	a10	a11	a12
a13	a14	a15	a16

Original State matrix

a1	a2	a3	a4
a6	a7	a8	a5
a11	a12	a9	a10
a16	a13	a14	a15

After NAES Shift

Fig 4: Shift Transformation

New AES algorithm is described below:
INPUT: Original Image, Secret Key
OUTPUT: Encrypted Image
METHOD: NAES(Original Image, Secret Key)
Step 1: Read the original image and divide the image into blocks of size 16×16.
Step 2: for each block repeat step 3 to 6.
Step 3: ADDROUNDKEY [Pre Initial Round]
Step 4: for round 1 to nr-1 do the following transformations:
- 4.1: SUBBYTE
- 4.2: NEW_SHIFT_ROW
- 4.3: MIX_COLUMNS
- 4.4: ADDROUNDKEY

Step 5: Perform following transformations [Final Round]
- 5.1: SUBBYTE
- 5.2: NEW_SHIFT_ROW
- 5.3: ADDROUNDKEY

Step 6: Combine all encrypted blocks to constitute encrypted image.

5. EXPERIMENTAL RESULTS

NAES image encryption algorithm is tested and evaluated on Matlab R2009b. Performance was measured on Intel(R) Core™ 2 Duo CPU T 5750 @ 2.00 GHz 2 GHz 32 bit system with 2 GB of RAM running Windows 7 Professional. We uses several images as original images (Plain Image). The Plain images and encrypted images are depicted in the Fig 5 and Fig 6.

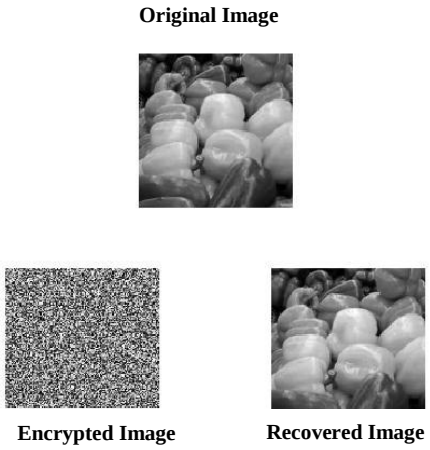

Fig 5: Application of NAES cipher to peppers.jpg

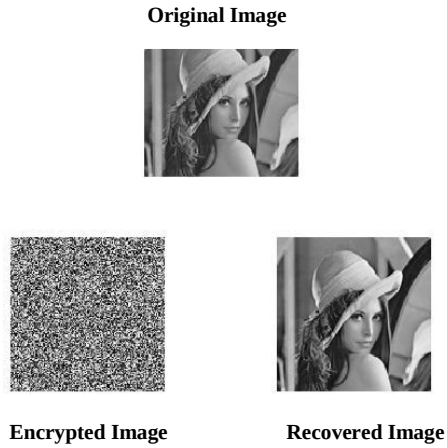

Fig 6: Application of NAES cipher to lena.jpg

6. STATISTICAL ANALYSIS

A good encryption scheme should refuse all kind of known attacks. Various security analysis has been performed on AES[9,14]. Shannon has suggested confusion and diffusion methods in order to discourage the attacks.

6.1 Histograms of Encrypted Images

An image can be represented graphically by number of pixels in an image using function of intensity. We have computed and analyzed the histograms of original image and encrypted image which shows the drastically different content

We have calculated and analyzed the histograms of several encrypted images as well as original images which have totally different content as shown in Fig 7. The histogram of plain image (peppers.jpg) (size 128*128) has large spikes. The histogram of encrypted image is totally different. It is clear from the histograms of plain and cipher image that there is no resemblance between original and encrypted image. Hence does not provide any clue to employ statistical attack on proposed image encryption procedure.

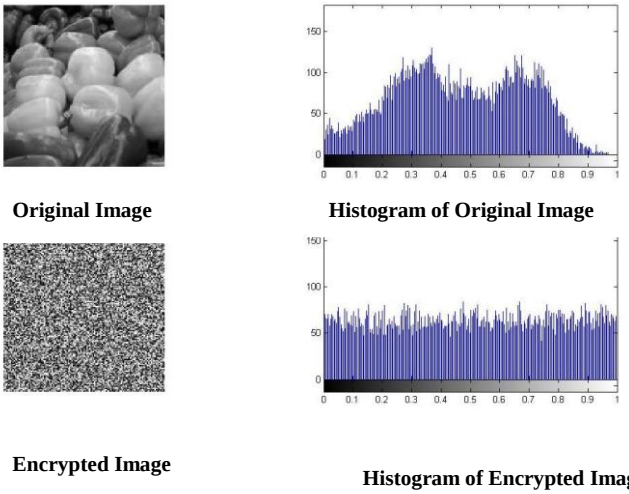

Fig 7: Histogram of Plain Image and Cipher Image

6.2 Correlation of Two Adjacent Pixels

We calculated correlation between adjacent pair of pixels in three directions: horizontal, vertical and diagonal. First, we randomly select n pair of two adjacent pixels from an image, then the correlation coefficient is calculated by using the following formula:

$$Cov(x,y) = E[(x - E[x])(y - E[y])]$$

$$rxy = cov(x,y) \div \sqrt{D(x)D(y)}$$

Where x and y are gray scale values of two adjacent pixels in the image.

Table 2 Correlation Coefficient of adjacent pixels in Original and Encrypted Image

Image Size	Direction	Plain Image	Cipher Image	
			AES	NAES
128*128	Horizontal	0.90006	0.01074	**0.00758**
	Vertical	0.9503	-0.0108	**-0.0111**
	Diagonal	0.8553	-0.0015	**-0.0036**
256*256	Horizontal	0.9483	0.00242	**-0.00494**
	Vertical	0.9708	-0.0018	**-0.00488**
	Diagonal	0.9221	-0.0028	**-0.00464**
512*512	Horizontal	0.9797	0.00984	**-0.13986**
	Vertical	0.9891	0.0079	**-0.02898**
	Diagonal	0.9672	0.00078	**-0.0992**

6.3 Image Quality Measures

The phrase Peak Signal to Noise Ratio, abbreviated as PSNR, is an engineering term for the ratio between maximum possible power of signal and the power of corrupting noise that affects the fidelity of its representation. The PSNR is most commonly used as measure of quality of reconstruction of an image[15]. The signal in this case is original image and noise is the distortion introduced by encryption. A higher PSNR normally indicate that reconstruction is of high quality. Mathematically PSNR is given by:

$$PSNR = 10\log_{10}\frac{1}{MSE}(dB)$$

Where MSE[16] is Mean Square Error computed as:

$$MSE = (1 \div MN)\sum_{i=1}^{MN}(o_i - d_i)^2$$

Where o_i and d_i are original image and distorted(cipher) image pixels respectively and M*N is the size of image. We take several size of images to test the NAES performance. It is clear from the table that lesser MSE is obtained from NAES which demonstrates the better performance of NAES than AES.

Table 3 Image Quality Measures of Original and Encrypted Image

Image Size	Parameter	AES	NAES
128*128	MSE	0.1169	0.1168
	PSNR	57.4570	57.4571
	N-Cross Correlation	0.9271	0.9181
256*256	MSE	0.1190	0.1188
	PSNR	57.3771	57.3814
	N-Cross Correlation	0.9165	0.9152
512*512	MSE	0.1193	0.1191
	PSNR	57.3649	57.3699
	N-Cross Correlation	0.9146	0.9163

7. CONCLUSION

In this paper new modified version of AES, to design secure symmetric image encryption scheme has been proposed. The modification is done by adjusting the shift row transformation of AES. No extra function is added to the original AES. It has been seen that the NAES performs better than AES in terms of statistically correlation and image quality measure. Future work may involve combining the NAES with steganography technique in order to accomplish data hiding and to provide more security against various known attacks.

8. REFERENCES

[1] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice-Hall, New Jersey, 1999.

[2] B. Schneier, "Applied Cryptography", John Wiley & Sons Inc., 1999.

[3] Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill Education, 2011.

[4] R. C. Gonzalez and R. E. Woods, "Digital Image Processing", Reading. MA:Addison Wesley, 2004.

[5] "Digitizing", "wikipedia.org", [online] Available at: http://en.wikipedia.org/wiki/Digitizing.

[6] "AES", "wikipedia.org", [online] Available at: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[7] Federal Information Processing Standards Publication 197(FIPS197), http://csrc.nist.gov/publications/fips/fips197/fips- 197.pdfS, 2001.

[8] J. Daemen, V. Rijmen, The block cipher Rijndael, Smart Card Research and Applications (2000) 288–296.

[9] An J.J. Amador, R. W.Green "Symmetric-Key Block Cipher for Imageand Text Cryptography": International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188.

[10] Seyed Hossein Kamali, Reza Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", IEEE Electronics and Information Engineering International Conference (ICEIE 2010). 1-3 Aug. 2010, V1-141 - V1-145.

[11] Shannon CE., "Communication theory of secrecy system," Bell SystTech J 1949;28:656-715.

[12] Ratinder Kaur, V. K. Banga "Image Security using Encryption based Algorithm": International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP'2012) July 15-16, 2012 Singapore.

[13] Abdelfatah A. Yahya and Ayman M. Abdalla"A Shuffle Image-Encryption Algorithm"Department of Computer Science, Al-Zaytoonah University of Jordan, Journal of Computer Science 4 (12): 999- 1002, 2008.

[14] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki "A Modified AES Based Algorithm for Image Encryption": Proceeding of the World Academy of Science, Engineering and Technololgy, May, WASET Organization, USA,2007.

[15] "PSNR", "wikipedia.org", [online] Available at: http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

[16] "MSE", "wikipedia.org", [online] Available at: http://en.wikipedia.org/wiki/Mean_squared_error.