Performance Evaluation of a New AES Based Image Encryption Technique

Chandra Prakash Dewangan, Shashikant Agrawal

Dept. of Electronics and Telecommunication Chhatrapati Shivaji Institute of Technology, Durg, India,

Abstract
In the era of computer and internet technology, multimedia protection is becoming increasingly jeopardized. Therefore numerous ways of protecting information are being utilized by individuals, businesses and governments. This paper mainly focuses on a new AES based image encryption technique using binary code which is expected to provide safety of images travelling over the internet. In order to evaluate the performance, the proposed image encryption technique was measured through a series of tests. These tests included a histogram analysis, information entropy, correlation analysis and differential analysis. Experimental results showed that the proposed encryption technique has satisfactory security and is more efficient than using the AES algorithm alone which makes it a good technique for the encryption of multimedia data. The results showed that the histogram of an encrypted image produced a uniform distribution, which is very different from the histogram of the plain image, and the correlation among image pixels was significantly decreased by using the proposed encryption technique and higher entropy was achieved.

Keywords
Advanced Encryption Standard (AES), Avalanche Effect, Cipher Text, Secret Key

I. Introduction
Data encryption is a product of the information theory area of mathematics, an area that addresses various ways to manage and manipulate information. Cryptography contains two basic processes: one process is when recognizable data, called plain data or plaintext, is transformed into an unrecognizable form, called cipher data or ciphertext. To transform data in this way is called to encipher the data or encryption. The second process is when the cipher data is transformed back to the original plain data, this is called to decipher, or decrypting the data. To be able to determine if a user is allowed to access information a key is often used. Once a key has been used to encipher information, only someone who knows the correct key can decipher the encrypted data. The key is the foundation of most data encryptions algorithms today. A good encryption algorithm should still be secure even if the algorithm is known [1-3, 11-12]. Encryption is the process of scrambling the information to insure its security. With the huge growth of computer networks and internet technology, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. As a result, different security techniques have been used to provide the required protection [4]. With the advancements of multimedia and networks technologies, a vast number of digital images now transmitted over Internet and through wireless networks for convenient accessing and sharing [12]. Due to some inherent features of images like bulk data capacity and high data redundancy, the encryption of images is different from that of texts; therefore it is difficult to handle them by traditional encryption methods. In this paper, a new image encryption algorithm based on binary mapping maps is proposed. The rapid growth in the computer and internet technology leads a common tradition for interchanging of the digital images very drastically. Hence it is more vulnerable of duplicating of digital image and re-distributed by hackers. Therefore the image has to be protected while transmitting it. Sensitive information like credit cards, banking transactions and social security members need to be protected. Various encryption techniques for this purpose are existing which are used to avoid the information theft. In recent days of internet, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. Different encryption techniques are used to protect the confidential data from unauthorized access.

II. Related Work
Mohammad Ali Bani Younes and Aman Jantan [4] further presented another algorithm for image encryption in April 2008, which was a combination of a permutation technique followed by encryption. It introduced a new technique based on the combination of permutation image encryption and a well-known algorithm known as Rijndael. The original image was divided to blocks of 4 pixels by 4 pixels, which were reorganized into a permuted image through a process of random permutation. Then the generated image was encrypted using the Rijndael algorithm. The results showed that the correlation between the elements of the image had been significantly reduced by using the technique of combination and higher entropy was obtained.

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra and Ganapati Panda [6] proposed an algorithm called Advanced Encryption Hill (AdvHill) that used a matrix of encryption key involution. They took different pictures and encrypted them using the original Hill cipher algorithm and the proposed AdvHill algorithm. It was evident that the original Hill cipher could not properly encrypt the images if the image consists of a large surface covered with the same colour or grayscale. However, the proposed algorithm worked for all grayscale images, and images of different colours.

Shesha Pallavi Indrakanti and P.S. Avadhani [7] proposed a new image encryption algorithm based on random permutation pixels with the motivation to maintain image quality. The technique had three distinct phases in the process of encryption. The first phase was the image encryption. The second phase was the phase of key generation. The third phase was the process of identification. This guaranteed confidentiality for colour images with less calculation and the process of permutation was much faster and efficient. The key generation process was unique and was a different process. Rasul Enayatifar, Abdul Hanan Abdullah [8] proposed a new method based on a hybrid model consisting of a genetic algorithm and an encryption based on the chaotic function applied to an image. In their technique, first a number of encrypted images were built using the original image with the help of the chaotic function. In the next step, encrypted images were used as the initial population to start the operation of the genetic algorithm. Then the genetic algorithm was used to optimize the encrypted...
images as much as possible. Ultimately, a good cipher image was selected as the final image encryption. Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [13] proposed a new algorithm for image encryption based on the SHA-512 hash function. The algorithm consisted of two main sections: The first pre-treatment was to mix only half the picture. The second section used the hash function to generate a mask of random numbers. The mask was then XOR’d with the other side of the image that was encrypted. 

Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [15] proposed a two-phase encoding and decoding algorithm based on shuffling the pixels of the image using the affine transformation followed by encryption of the resulting image using the XOR operation. To redistribute the pixel values in the different locations the technique used the affine transformation with four 8-bit keys. The transformed image was split into 2 pixel x 2 pixel blocks and each block was encrypted using the XOR of four 8-bit keys. The total size of the key used in the algorithm was 64 bits. Their results showed that after the affine transformation of the image the correlation between pixel values had been reduced considerably.

In order to decrease the high correlation among pixels and increase the entropy value of an image, we propose a process based on mapping the image using the different binary codes. The generated image is then fed into the AES encryption algorithm. By using a histogram, the correlation, entropy, MAE, NPCR, and UACR as measures of testing the security, the shifting process and the subsequent technique will be expected to result in a different histogram, a lower correlation, a higher entropy value, and thus an improved security level of the encrypted images, i.e., by using analysis of MAE, NPCR and UACR.

III. Methodology

In the proposed algorithm we have changed the form of plain image (i.e. the input image) and encryption key given to the AES algorithm. Instead of giving plain image and Encryption key directly to the AES algorithm, we have mapped input plain image and input encryption key in various binary codes before being applied to the input of the AES algorithm. Some of these binary codes are weighted and some are unweighted. [11] fig. 1 shows the standard AES process while fig. 2 shows the block diagram of algorithm that we have used for our experiments.

If there are n quantities in a group, a code of binary digits or bits may represent all quantities unequally.

\[ N \leq 2^n \]

A. Natural BCD Code (8421 code)

Natural BCD code or 8421 code is used whenever decimal information is transferred in or out of a digital system. In this code straight assignment of binary equivalent is used with weights.

B. 2421 Code

These are weighted, reflected and self-complementing codes. In 2421 codes if a number has more than one representation then choose the code uses the lower binary weights (for number 0-4 only).

C. 5421 Code

These are weighted code with weight 5-4-2-1. In 5421 codes if a number has more than one representation then choose the code that uses the lower binary weights.

D. 7421 Code

These are weighted code with weight 7-4-2-1. For decimal number 7 choose code with least number of 1’s.

E. 5311/5211 Code

These are weighted code with weight 5-3-3-1. In 5311 codes if a number has more than one representation then choose the code with least number of 1’s and use first the 1 from extreme right that uses the lower binary weights.

F. Gray code

It is also known as “reflected and unit distance code” which is a reflected mirror image. Unit distance exhibit only a single bit change from one code to the next. It is also an unweighted and not an arithmetic code.
G. 3321/4221 Code
These are weighted code with weight 3-3-2-1/4-2-2-1.[20]

IV. Experimental Result
The proposed image encryption algorithm is tested and evaluated based on software simulation. Results of some experiments are given to prove its effectiveness in application to digital image. We use several images as the original images (plain images). The encrypted images are depicted in Figure 3. As shown, the encrypted images (cipher image) regions are totally invisible. The decrypted images are shown in Figure. The visual inspection of Figure 3 shows the possibility of applying the proposed successfully in both encryption and decryption. Also, it reveals its effectiveness in hiding the information contained in them.

V. Security Analysis
In order to resist statistical attacks, the encrypted images should acquire certain random properties. A statistical analysis has been performed To show the robustness of the proposed algorithm, by calculating the histograms, the correlations analysis of adjacent pixels for the plain image and the encrypted image. Experiment have been performed of different images and it has been determined that the intensity values are good.

A. Key Space Analysis
Key space size is the total number of different keys that can be used in the encryption. For a secure image encryption, the key space should be large enough to make brute force attacks infeasible [14]. The proposed cipher has $2^{128}$ different combinations of the secret key. An image cipher with such a long key space is sufficient for reliable practical use.
To prevent the information containing the original image from an opponent, it is also beneficial that cipher image bears little or no statistical similarities to the plain image. An image histogram is a most commonly used method of analysis in image processing and data mining applications. The advantage of a histogram is that it shows the shape of the distribution for a large set of data. Thus, an image histogram illustrates how the pixels in an image are distributed by graphing the number of pixels at each color intensity level. It is important to ensure that the encrypted and original images do not have any statistical similarities. The histogram analysis clarifies how pixels in an image are distributed by plotting the number of pixels at each intensity level.

The experimental results of the plain image and its corresponding cipher image and their histograms are shown in fig. 4. The histogram of each plain image illustrates how the pixels are distributed by graphing the number of pixels at every grey level. It is clear that the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the respective histograms of the original images.

C. Correlation of Two Adjacent Pixels

In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain-image/cipher image respectively. The procedure is as follows: First, randomly select 3000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following formula:

\[ C_r = \frac{N \sum_{i=1}^{N} (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{N \sum_{i=1}^{N} (X_i - \bar{X})^2 \sum_{i=1}^{N} (Y_i - \bar{Y})^2}} \]

Where \( x \) and \( y \) are the intensity values (are grey-scale values) of two neighboring pixels in the image and \( N \) is the number of adjacent pixels selected from the image to calculate the correlation.

D. Entropy

Information theory is the mathematical theory of data communication and storage founded in 1949 by C.E. Shannon [19]. Modern information theory is concerned with error-correction, data compression, cryptography, communications systems, and related topics. To calculate the entropy \( H \) of a source \( m \), we have:

\[ H(m) = -\sum_{i=0}^{2^{N-1}} p(m_i) \log_2 \frac{1}{p(m_i)} \]

Where \( p(m_i) \) represents the probability of symbol \( m_i \) and the entropy is expressed in bits. Let us suppose that the source emits 28 symbols with equal probability, i.e., \( 1 \leq 28 \quad m = \{ m, m, \ldots, m \} \) after evaluating Eq. (2), we obtain its entropy \( H(m) = 8 \), corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. Let us consider the ciphertext of image encryption using the proposed block cipher, the number of occurrence of each ciphertext block is recorded and the probability of occurrence is computed. We illustrate the entropy analysis of our scheme kept at the same word size \( w=32 \), number of rounds \( r=10 \), and secret key length \( b=16 \) respectively, and compare it with other schemes. Table 3, indicates the various values of the entropies for encrypted images.

E. Differential Analysis

In general, a desirable property for an encrypted image concerns its sensitivity to small changes in the plain-image (e.g., modifying only one pixel). An opponent attempting to crack the encryption can create a small change in the input image to observe changes in the result. By this scheme, a meaningful relationship between the original image and the encrypted image can be simply found. If one small change in the plain image can cause a significant change in the cipher image, with respect to diffusion and confusion, then the differential attack actually loses its efficiency and becomes practically useless. Three common measures have been used for differential analysis: MAE, NPCR and UACI [16-18]. MAE stands for mean absolute error. NPCR is the number of pixel change rate of the ciphered image when one pixel of the plain image is changed. The Unified Average Changing Intensity (UACI) measures the average intensity of the differences between the plain image and the ciphered image. Let \( C \) and \( P \) be the grey levels of the pixels at the ith row and jth column of a \( W \times H \) cipher and plain image, respectively. The MAE between these two images is obtained from Equation 3:

\[ MAE = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} |C(i,j) - P(i,j)| \]

Consider two cipher images \( C_1 \) and \( C_2 \), whose corresponding plain images have only one pixel difference.then the NPCR of these two images is defined using Equation 4:

\[ NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \]
Where $W$ and $H$ are the width and height of the image $(i,j)$ is defined using equation (5):

$$D(i,j) = \begin{cases} 0 & \text{if } C_2(i,j) = C_2(i,j) \\ 1 & \text{if } C_2(i,j) \neq C_2(i,j) \end{cases}$$

Another measure is UACI, which is defined using Equation (6):

$$UACI = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} \left( \frac{|C_2(i,j) - C_{2}(i,j)|}{255} \right) \times 100\%$$

### Table 3: Result for Differential Analysis

<table>
<thead>
<tr>
<th>Image</th>
<th>MAE</th>
<th>NPCR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>48.1868</td>
<td>99.6797%</td>
<td>26.7995%</td>
</tr>
<tr>
<td>Peppers</td>
<td>54.6771</td>
<td>99.7699%</td>
<td>27.8499%</td>
</tr>
</tbody>
</table>

Tests have been performed on the proposed technique on images of size 256×256 pixels. The results are given in Table 1, and 3. In order to evaluate the impact of changing one pixel in the plain image on the encrypted image, the NPCR, UACR, and MAE are calculated for the proposed technique. The results show that a small change in the original image will result in a significant difference in the cipher (encrypted) image. Therefore, the proposed scheme has a good ability to resist an anti-differential attack.

### VI. Conclusion

The proposed algorithm described in this paper has improved image security using gray code mapping and the standard AES algorithm. It is very important to impact the correlation among image pixels in a plain image to increase the security level of the encrypted image. The proposed algorithm is expected to show good performance, uniform distribution in a histogram, a low correlation and a high entropy. To quantify the difference between the encrypted image and the corresponding plain-image, three measures were used: MAE, NPCR, and UACI. The results show that a small change in the original image will result in a significant difference in the cipher image. Consequently, experimental results show that the proposed algorithm has a high security level. It can withstand against known and chosen plain text, brute force, statistical and differential attacks, and is able to encrypt large data sets efficiently. The proposed method is expected to be useful for real-time image encryption.

### References


Chandra Prakash Dewangan received his B.Sc. degrees in Electronics from Pt. Ravi Shankar Shukla University, Raipur in 2004 and completed M.Sc. degrees in Electronics from S.O.S. in Electronics, Pt. Ravi Shankar Shukla University, Raipur, India, and 2006. He is pursuing his M.E. degree at Chhattisgarh Swami Vivekanand Technical University, Bhilai. His area of research includes cryptography and network security. He is a student member of Institute of Electrical and Electronics Engineers (IEEE).

Prof. Shashikant Agrawal received his B.E degree in Electronics and Telecommunication from Pt. Ravi Shankar Shukla University, Raipur, in 2007 and completed his post graduation from Swami Vivekananda Technical University, Bhilai in 2011. He is currently serving as Assistant professor in the department of Electronics and Telecommunication, Chhatrapati Shivaji Institute of Technology, Durg. His areas of interest include image processing and Information Security. He is a life member of Indian Society for Technical Education.