International Journal of Cryptography and Security
ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-32-35.
Available online at http://www.bioinfo.in/contents.php?id=115

CRYPTOGRAPHY USING AES ALGORITHM

BHUSHAN SHINDE, SHRADDHA JAISWAL, PRASANNA GULHANE AND NILIMA SHETE

Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India.
*Corresponding Author: Email- bhushan.shinde93@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- With the fast evolution of digital data exchange,security information becomes much important in data storage and transmission. Due to the increasing use of images in industrialprocess, it is essential to protect the confidential image data fromunauthorized access. In this paper, we analyze the Advanced Encryption Standard (AES), and we add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance; mainly for images characterised by reduced entropy.Comparative study with traditional encryption algorithms is shown the superiority of the modified algorithm. Detailed results in terms of security analysis and implementation are given. Comparative study with traditional encryption algorithms is shown the superiority of the modified algorithm.
Keywords- Cryptography, Encryption, Advanced Encryption Standard (AES), ECB mode, statistical analysis,key stream generator

Citation: Bhushan Shinde, et al. (2012) Cryptography Using Aes Algorithm. International Journal of Cryptography and Security, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, pp.-32-35.

Introduction

It is a common technique to uphold image security. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Telemedicine and military communication.Many image-protection techniques are using vector quantization (VQ) as encryption technique (Chang et al., 2001; Chen and Chang, 2001). In Chang et al. (2001), VQ decomposes an image into vectors, which are then encoded and decoded vector-by-vector. Alternatively, Chen and Chang (2001) use VQ to divide desired images for encryption into a large number of shadows that are guaranteed undetectable to illegal users. Image and text cryptography has been achieved using chaotic algorithms (Fridrich, 1997; Sobhy and Shehata, 2001, Haojiang, Yisheng, Shuyun and Dequn Li 2005). A symmetric block encryption algorithm creates a chaotic map (Fridrich, 1997) for permuting and diffusing image data. For thorough encryption, the chaotic map is applied to the image, iteratively, multiple times. The chaotic algorithm of Sobhy and Shehata (2001) is based on the Lorenz system of equations. Both image and text data are encrypted successfully, but knowledge of the system allows devising anoptimization routine that discovers the key by output minimization.

Related work

Phase encoding techniques exist for encrypting image data (Zhang and Karim, 1999; Park et al., 2001). Color image data is regarded in Zhang and Karim (1999), where a double-phase technique is utilized. Color images are encrypted from an indexed image and thereby decrypted back to its color format. The work of Wu and Kuo (2001) describes selective encryption based on a digital coefficients table. It was shown its limitation due to a less intelligible recovered image. Color and gray-scale images were considered in Koga and Yamamoto (1998), where a lattice-based extension to Visual Secret Sharing Scheme (VSSS) (Naor and Shamir, 1994) was developed. A hashing approach to image cryptography is taken in Venkatesan et al. (2000); wavelet representations of images are obtained, and a new randomized strategy for hashing is introduced. Several cryptosystems exist like as data encryption [3], steganography [14], digital signature (Aloka Sinha, Kehar Singh, 2003) and SCAN (S.S. Maniccama, N.G. Bourbakis

2004) have been proposed to increase the security of secret images. However, one common defect of these techniques is their policy of centralized storage, in that an entire protected image is usually maintained in a single information carrier. abnormality in the information carrier in which the protected image resides, he or she may intercept it, attempt to decipher the secret inside or simply ruin the entire information carrier (and once the information carrier is destroyed, the secret image is also lost forever). Another method is to encrypt image data, e.g., using DES (Data Encryption Standard). DES, however, is very complicated and involves large computations. A software DES implementation is not fast enough to process the vast amount of data generated by multimedia applications and a hardware DES implementation (a set-top box) adds extra costs both to broadcasters and to receivers. In order to tackle these problems systems based on advanced encryption standard (AES) where proposed. AES is very fast symmetric block algorithm especially by hardware implementation [7, 11, 12, 15]. The AES algorithm is used in some applications that require fast processing such as smart cards, cellular phones and image-video encryption. However, a central consideration for any cryptographic system is its susceptibility to possible attacks against the encryption algorithm such as statistical attack, differential attack, and various brute attacks. Block cipher symmetric algorithms; allow different ciphering mode [17]. Electronic CodeBook (ECB) is the most obvious mode; ciphered blocks is a function of the corresponding plaintext block, the algorithm and the secret key. Consequently a same data will be ciphered to the same value; which is the main security weakness of that mode [1, 15, 19, 20]. CBC mode provides improved security since each encrypted block depends also on the previous plaintext block. Its use proves limited in an encryption image due to the processing time. There are two levels of security for digital image encryption: low-level security encryption and highlevel security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable at all to the viewers. This paper proposes new encryption schemes as a modification of AES algorithm. The modification is done by adding a key stream generator, such as (A5/1, W7), to the AES image encryption algorithm in order to increase the image security and in turn the encryption performance.

AES Algorithm

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) [4, 6].These rounds are governed by the following transformations:

Bytesub transformation: Is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation. The Fig. 1 shows the step of the Bytesub transformation.

Shiftrows transformation: Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.

Mixcolumns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

Addroundkey transformation: Is a simple XOR betweenthe working state and the roundkey. This transformation is its own inverse.

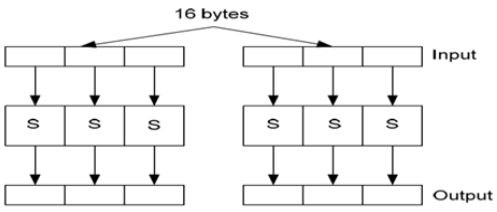


Fig. 1- Block diagrams for Substitution

The encryption procedure consists of several steps as shown by Fig. 2- After an initial addroundkey, a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (Nr times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Bytesub, the Inv-Shiftrows, the Inv-Mixcolumns, and the Addroundkey allow the form of the key schedules to be identical for encryption and decryption.

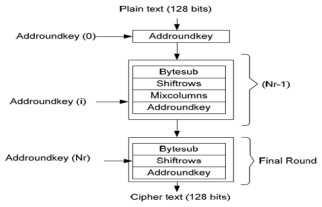


Fig. 2- AES algorithm- Encryption Structure

Security analysis by statistical approach

A good encryption scheme should resist all kinds of known attacks, such as known-plain-text attack, cipher-text attack, statistical attack, differential attack, and various brute-force attacks. Some security analysis techniques perform on the AES image encryption scheme, including the statistical analysis and key space analysis.

Statistical Analysis

Shannon suggested two methods of diffusion and confusion in order to frustrate the powerful attacks based on World Academy of Science, Engineering and Technology 27 2007 statistical analysis [18]. Statistical analysis has been performed on the AES, demonstrating its superior confusion and diffusion properties which strongly defend against statistical attacks. This is shown by a test on the histograms of the enciphered image and on the correlation of adjacent pixels in the ciphered image.

Histogram of encrypted image

We select several grey-scale images (256×256) having different contents, and we calculate their histograms. One typical example

among them is shown in Fig. 3. We can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. Therefore, it does not provide any indication to employ any statistical attack on the image under consideration. Moreover, there is no loss of image quality after performing the encryption/decryption steps [9].

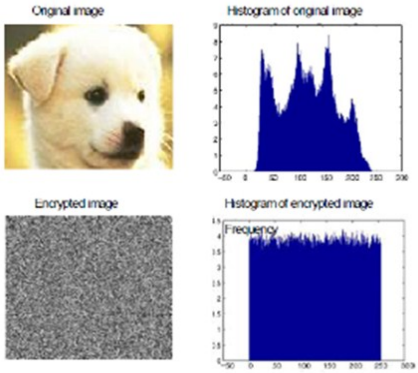


Fig. 3- Histograms of the plain image and ciphered image

Correlation of two adjacent pixels

We test the correlation between two vertically adjacent pixels, and two horizontally adjacent pixels respectively, in a ciphered image. First, we randomly select n pairs of two adjacent pixels from an image. Then, we calculate the correlation coefficient of each pair by using the following formula.

$$cov(x,y) = E(x - E(x))(y - E(y)) \quad (1)$$

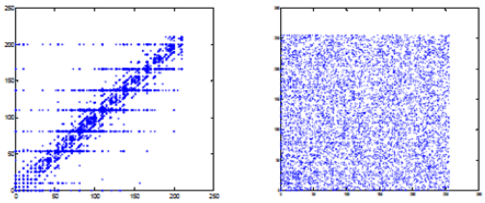
Where x and y are grey-scale values of two adjacent pixels in the image. Figs. 4(a)-(b) show the correlation distribution of two horizontally adjacent pixels in the plain-image and in the ciphered image, respectively. Simulation results for horizontal and vertical directions were illustrated in Table I.

VKEY Space analysis

A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make bruteforce attacks infeasible [16, 5, 10]. In our case, the key space size is 10128. It is large enough to resist at all type of bruteforce attacks. The experimental results also demonstrate that AES is very sensitive to the secret key. Table I illustrates the sensitivity of AES to the secret key ki. Fig. 4(a) shows Lenaimage encrypted using different ki. As can be seen when the secret key ki is changed slightly the encrypted image becomes absolutely different. Similar results can be obtained for correlation coefficients as shown in Table II. As we can see, the sensitivity to key which is the main characterization of AES algorithm guarantees the security of our scheme. Undoubtedly, the secret keys are secure enough even when a chosen plaintext/ciphertext attack is adopted.

Table 1-Correlation Coefficient of Two Adjacent Pixel in Two Image (Lena Test Image Encrypted Using Different KI)

Correlation	Horizontal	Vertical
Plain image	0,93	0,95
Image encrypted by k1	0,058	0,051
Image encrypted by k2	0,036	0,035
Image encrypted by k3	0,047	0,044
Image encrypted by k4	0,06	0,054



(a) (b)

Fig. 4- Correlation of two horizontally adjacent pixels; (a) in the plain-image, and (b) in the ciphered-image

The AES image encryption system is analyzed thoroughly in this section. By studying the strengths of the confusion and diffusion properties, and its security against statistical attack, AES ensures a high security for ciphered image. But the security of the scheme is based on the complexity of AES and the image proprieties. In Electronic CodeBook (ECB) mode; ciphered block is a function of the corresponding plaintext block, the algorithm and the secret key. Consequently a same data will be ciphered to the same value; which is the main security weakness of that mode and the image scheme encryption. In fact, if the image contains homogeneous zones, all the same blocks remain also the same after ciphering. In this case encrypted image will also contain textured zones and the entropy of the image is not maximal. One typical example among them is shown in Fig. 5. A number of different objective measures can be utilized for quantitative comparison of the performance of the different algorithms. These criteria provide some measure of closeness between two digital images by exploiting the World Academy of Science, Engineering and Technology 27 2007 differences in the statistical distributions of the pixel values. In our study the following metrics have been used.

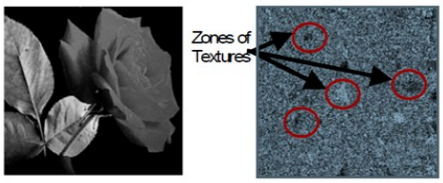


Fig. 5- Rose encryption - Appearance of textures zones

Modified AES Algorithm

This system helps diagnose engine troubles of certain models of Toyota cars developed by their research lab. Used in a central service department which can be called up by those actually servicing the cars for assistance, if required.

The new image encryption scheme is a modified AES algorithm. It is formed by the AES algorithm and a key stream generator as shown in Fig. 6. The latter has two different forms; (i) A5/1 key stream generator and (ii) W7 key stream generator.

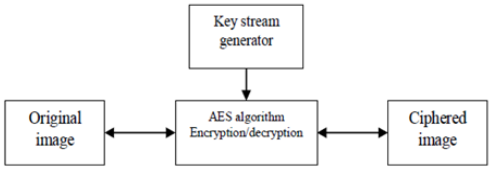


Fig. 6- New AES image encryption scheme

A5/1 KEY Stream generator

The A5/1 cipher is composed by three Linear Feedback Shift Registers (LFSRs); R1, R2, and R3 of length 19, 22, and 23 bits, respectively. Each LFSR is shifted, using clock cycles that are determined by a majority function. The majority function uses three bits; C1, C2, and C3. The 64 bits of the key map to the LFSR's initial state as: R1(19 bits): x19 + x5 + x2 + x + 1, R2(22 bits): x22 + x +1,R3(23 bits): x23 + x15 + x2 + x + 1. At each clock cycle, after the initialization phase, the last bits of each LFSR are XORed to produce one output bit [2, 8].

W7 Key stream Generator

The W7 algorithm is a byte-wide, synchronous stream cipher optimized for efficient hardware implementation at very high data rates. It is a symmetric key algorithm supporting key lengths of 128 bits. W7 cipher contains eight similar models; C1, C2,…., C8. Each model consists of three LFSR's and one majority function. W7 architecture is composed by a control unit and a function unit [8]. The function unit is responsible of the key stream generation. The proposed architecture for the hardware implementation of one cell is presented in Fig. 7. Each 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 of 1-bit long. The outputs of each cell form the keystream byte.

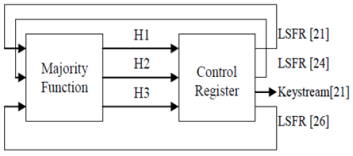


Fig. 7- W7 key stream generator proposed architecture

Conclusion

Scure symmetric image encryption technique, has been proposed. The AES is extended to support a key stream generator for image encryption which can overcome the problem of textured zones existing in other known encryption algorithms. Detailed analysis has shown that the new scheme offers high security, and can be realized easily in both hardware and software. The key stream generator has an important influence on the encryption performance. We have shown that W7 gives better encryption results in terms of security against statistical analysis attacks.

Result

Fig. 8- Image Encryption Result

Acknoledgement

We express our sincere gratitude to our guide, for his kind and able guidance for the completion of this paper. His consistent support and intellectual guidance made us to energize and innovate with new ideas.

References

[1] Bourbakis N., Dollas A. (2003) *IEEE Multimedia Mag*, 10, 79-87.
[2] Canteaut A. and Filiol E. (2000) *Technical report* 3887.
[3] Cheng H., Xiaobo L. (2000) *IEEE Trans. Signal Process*. 48 (8), 2439-2451.
[4] Daemen J., Rijmen V. (2000) *Third International Conference on smart card Research and Applications*, 1820, 277_284.
[5] Ferguson N., Kelsey J., Lucks S., Schneier B., Stay M., Wagner D.,Wagner D. and Whiting D. (2000) *Proceedings of Fast Software Encryption,* 213-230.
[6] (2001) *Federal Information Processing Standards Publications* (FIPS 197).
[7] Gaj K., Chodowiec P. (2001) *Fast implementation and fair comparison of the final candidates for advanced encryption standard using field programmable gate arrays*,.84-99.
[8] Galanis M.D., Kitsos P., Kostopoulos G., Sklavos N., Koufopavlou O. and Goutis C.E. *Comparison of the hardware architectures and FPGA implementations of stream ciphers*.
[9] Amador J.J., Green R.W. (2005) *International Journal of Imaging Systems and Technology*, 3, 2005, 178-188.
[10] Gilbert H. and Minier M. (2000) *The third Advanced Encryption Standard Candidate Conference*, 230- 241,*http://www.nist.gov/aes*.
[11] Hodjat A. and Verbauwhede I. (2004) 12*th Annual IEEE Symposium on Field-Programmable Custom Computing Machines*.
[12] Janvinen K., Tominisko M., Skytta J. (2003) *International symposium of Field programmable Gate arrays*, 207-215.
[13] Maniccama S.S., Bourbakis N.G. (2004) *Image and video encryption using SCAN patterns, in Pattern Recognition* 37, 725-737.
[14] Marvel L.M., Boncelet G.G., Retter C.T. (1999) *IEEE Trans. Image Process*, 8(8), 1075-1083.
[15] Mclone M., McCanny J.V. (2003) *J. VLSI signal process syst*. 34(3), 261-275.
[16] Phan R.C.W. (2004) *Information processing letters,* 91,33-38.
[17] Schneier B. (1996) *Algorithms and Source Code in C. John Wiley and Sons*.
[18] Shannon C.E. (1949) *Bell syst Tech*, 28, 656-715.
[19] Shiguo L., Jinsheny S., Zhiquan W. (2005) *A block cipher based a suitable of the chaotic standard map, chaos, solutions and fractals* 26, 117-129.
[20] Shujun L., Xuan Z., Xuanqin M., Yuanlong C. (2002) *chaotic encryption scheme for real time digital video, SPIE*4666, 149-160.