УДК 004.4

Ahmed H.H. Al-Furaiji,
Student,
Department "Big Data Analytics and Video Analysis Methods"
Engineering School of Information Technologies,
Telecommunications and Control Systems,
Ural Federal University named after the first President of Russia B.N. Yeltsin
Yekaterinburg, Russian Federation

Abdulkareem A.A. Al-Madani,
Student,
Department "Big Data Analytics and Video Analysis Methods",
Engineering School of Information Technologies,
Telecommunications and Control Systems,
Ural Federal University named after the first President of Russia B.N. Yeltsin
Yekaterinburg, Russian Federation

THE SMART STEGANOGRAPHY SYSTEM USING AES & SPK ALGORITHMS

Abstract:
In this paper a new steganography approach proposed based on LSB technique by using Alpha channel on JPG cover images and Bit-slicing decomposition and Advanced Encryption Standard (AES) on the secrete image. For this method first the secrete image decomposed to bit streams and the data encrypted using AES algorithm. On the cover side, an alpha channel is attached to the cover image and the data embedded into LSBs of RGBA channels. The method was implemented and tested by using MATLAB® (R2011a).

Keywords:
LSB, AES, Alpha channel, RGBA, Bit-slicing

Introduction

Steganography is an ancient art of hiding information in between other information that has been reborn in recent years [1]. A steganography system is expected to meet three key requirements, namely transparency, capacity, and robustness [2]. There are many steganographic methods, presented for example in [3,4].

The most suitable algorithm was created by Vincent Rijmen and Joan Daemen. They named it Rijndael after themselves [4]. On 26.11.2001 the Federal Information Processing Standards Publication (FIPS PUB 197) announced a standardized form of the Rijndael algorithm as the new standard for encryption called Advanced Encryption Standard (AES) [4]. The overall structure of AES can be seen in Fig. 1. The algorithm of its work is described in [5, 6].

There are many researches in the steganography techniques, and a brief description of some of them is presented in [7-9].

The proposed technique

While most of steganography techniques work on cover image or secrete image, our proposed technique relies on processing both of cover and secrete image to reach to the optimum results.

For the secrete image side the total data size is decreased, i.e. compressing the image to decrease the amount of the payload. Bit-plane slicing technique used to compress the secrete image and to convert it from 2D image to 1D bit stream. On the other side, working on the cover image to increase its ability to handle the payload. A fourth channel added to the JPG cover image to increase

the bit depth from 24 to 32, and to be four channels carrying the four-candidate bit-planes. The proposed system for the receiver side is shown in Fig. 2.

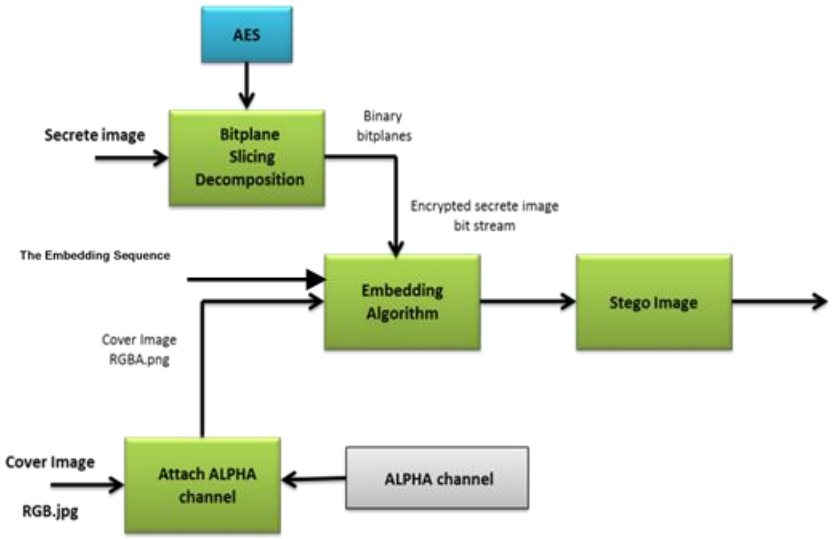

Figure 1 - The Main block diagram of the sender side

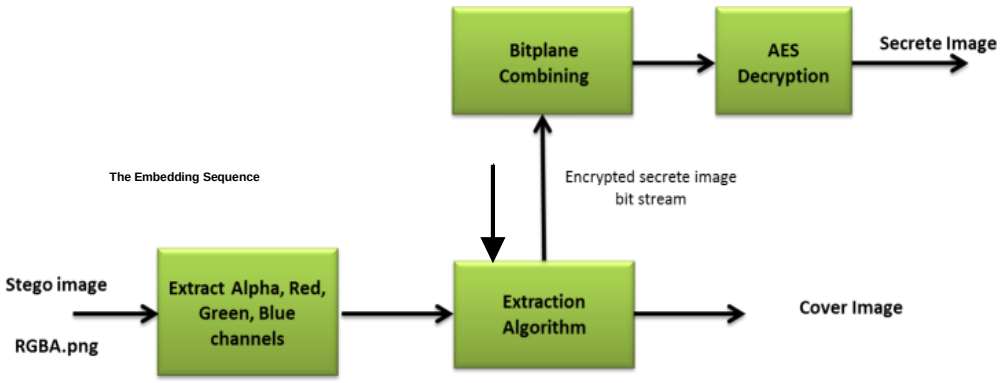

Figure 2 – Main block diagram of the receiver side

In this method, encryption is applied on the secrete image after taking the 4 upper bit-planes that selected from bit-plane slicing process. The 2D is encrypted before it converted to 1D array. The key used is 128 bits and number of rounds is 10 (Fig. 3).

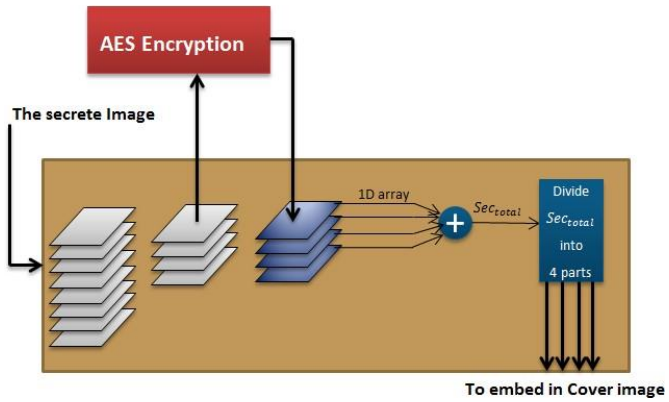

Figure 3 – The encryption of secrete image using AES algorithm

The S-box is constructed in the following fashion:

1. Initialize the S-box with the byte values in ascending order row by row. Thus, the value

of the byte at row x, column y is {xy}.

2. Map each byte in the S-box to its multiplicative inverse in the finite field GF(2^8), the value {00} is mapped to itself.

3. Consider that each byte in the S-box consists of 8 bits labeled (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0). Apply the affine transformation to each bit of each byte in the S-box:

$$b_i' = b_i \oplus b_{(i+4) mod 8} \oplus b_{(i+5) mod 8} \oplus b_{(i+6) mod 8} \oplus b_{(i+7) mod 8} \oplus c_i$$

(18) where c_i is the i^{th} bit of byte c with the value {63}, that is, ($c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0$) = (01100011). The prime (′) indicates that the variable is to be updated by the value on the right.

The AES standard depicts this transformation in matrix form as follows: $_0$ {95}$^{-1}$ = {8a}, which is 10001010 in binary. Using equation (3.21), the result is {2A}.

Proposed Embedding Algorithm

In this algorithm, a secret image will be hidden in a cover image using LSB. Embedding operation is variable. The number of LSB bits used to embed can vary from 1 bit to 8 bits. This embedding sequence is chosen by the sender.

Results and discussion

A series of experiments have been conducted to show the effectiveness of the proposed technique. The efficiency of the proposed technique is measured by Five metrics which are:

- PSNR (Peak Signal-to-Noise Ratio);
- MSE (Mean Square Error);
- Normalized Cross Correlation;
- AD (Average Difference);
- Histogram Analysis.

Two types of perceptibility can be distinguished and evaluated in signal processing systems, namely fidelity and quality. Fidelity means the perceptual similarity between signals before and after processing. However, quality is an absolute measure of the goodness of a signal.

To evaluate the performance of the proposed system in term of invisibility, a comparison between the proposed method and [3, 8, 12, 13, 14] is shown in Table 1.

Table 1 – The comparison of PSNR between the proposed system and other methods

Method	**Ref. [3]**	**Ref. [13]**	**Ref. [17]**	**Ref. [20]**	**Ref. [21]**	**Ref. [22]**	**Proposed**
PSNR	36.493	41.948	42.778	31.271	41.32	37.551	43.997

The Security of the proposed system:

In fact, there are no possible attack on AES better than brute-force attack. Assuming a computer that try keys at the rate of one billion keys per second. Under this assumption, the attacker will need about 10 000 000 000 000 000 000 000 (10 billions trillions) years to try all possible keys for the version AES-128 [15].

The way that the AES encrypt the secret image also gives a degree of invisibility and robustness beside the high degree of security, where the extracted encrypted image (in the case of detection and successful extraction) is look like a random image (or insignificant data) while there is no sign that the extracted image is actually a secret encrypted image. The attacker cannot distinguish between the encrypted image and any randomized pixel's values image.

Conclusions

1. A new data hiding technique presented, that allows hiding a colour image (secret object) in another colour image (cover object), achieving up to 100% embedding capacity.

2. The use of AES algorithm as an encryption method level up the security of the system

to high degree. Statistical results show that the system has high invisibility.

3. Using Bit-Slicing technique compresses the secrete image, and this results in decreasing the total amount of data embedded.

4. Attaching the alpha channel to the RGB image increases the bit depth of the image and this results in increasing the embedding range.

5. Alpha channel can handle more bits than the other channels while maintain a good PSNR considering that the Alpha channel is the lowest byte of the RGBA pixel.

References:

1. S.A. Laskar, and K. Hemachandran, Secure Data Transmission Using Steganography and Encryption Technique, International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.3, September 2012.
2. V.K. Mann, and H.S. Dhaliwal, 32×32 Colour Image Steganography, International Journal of Engineering Trends and Technology (IJETT), Volume 4, Issue 8, August 2013.
3. R.C. Gonzalez, and R.E. Woods, Digital Image Processing, 3rd edition, Prentice Hall, Upper Saddle River, 2008.
4. Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November, 2001.
5. K. Kamalam, and S. Saranya, An Effective Method in Steganography to Improve Protection Using Advanced Encryption Standard Algorithm, International Journal of Engineering Trends and Technology (IJETT), Volume 18, Number 4, Dec 2014.
6. H. Sajedi, and M. Jamzad, Secure steganography based on embedding capacity, Springer-Verlag, International Journal of Information Security, volume 8, Issue 6, 2009.
7. A. Cheddad, "Steganoflage A New Image Steganography Algorithm ", PhD Thesis, School of Computing & Intelligent Systems Faculty of Computing & Engineering University of Ulster, September 2009.
8. S. Khaire, et. al., Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique, International Journal of Engineering Science and Technology, Volume 2, Issue 9, 2010.
9. A.J. Sadiq, Comparison Steganography in spatial domain of Image, Journal of Baghdad College of Economic Sciences, No.29, Baghdad, 2012.
10. S. Venkatraman, A. Abraham, and M. Paprzycki, Significance of Steganography on Data Security, The International Conference on Information Technology : Coding and Computing, ITCC 2004.
11. Z.N. Abdulhameed, and M. K. Mahmood, High Capacity Steganography based on Chaos and Contourlet Transform for Hiding Multimedia Data, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 5, Issue 1, January 2014.
12. M. Niimi, H. Noda, E. Kawaguchi, and R. O. Eason, High Capacity and Secure Digital Steganography to Palette-Based Images, IEEE, 2002.
13. S.A. Parah, and J.A. Sheikh, Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique, IEEE, International Conference on Emerging Trends in Science, Engineering and Technology, 978-1-4673-5144-7/12, 2012.
14. K.B. Raja, S. Sindhu, and T.D. Mahalakshm, Robust Image Adaptive Steganography using Integer Wavelets, IEEE Image Processing, 2011.
15. A.W. Naji, et al., Novel Framework for Hidden Data in the Image Page within Executable File Using Computation Between Advance Encryption Standard and Distortion Techniques, International Journal of Computer Science and Information Security (IJCSIS), Volume 3, No. 1, Aug 2009