PAPER • **OPEN ACCESS**

Hiding Techniques for Dynamic Encryption Text based on Corner Point

To cite this article: Firas A. Abdullatif *et al* 2018 *J. Phys.: Conf. Ser.* **1003** 012027

Hiding Techniques for Dynamic Encryption Text based on Corner Point

Firas A. Abdullatif[1], Alaa A. Abdullatif[2], Amna al-Saffar[3]

[123]University of Baghdad\College of Education for pure science-Ibn Al-Haitham\computer science department

Firas.alobaedy@gmail.com, Alaa_3b@yahoo.com,
Amnaalsafar1@yahoo.com

Abstract. Hiding technique for dynamic encryption text using encoding table and symmetric encryption method (AES algorithm) is presented in this paper. The encoding table is generated dynamically from MSB of the cover image points that used as the first phase of encryption. The Harris corner point algorithm is applied on cover image to generate the corner points which are used to generate dynamic AES key to second phase of text encryption. The embedded process in the LSB for the image pixels except the Harris corner points for more robust. Experimental results have demonstrated that the proposed scheme have embedding quality, error-free text recovery, and high value in PSNR.

Keywords: steganography, Harris corner point algorithm, dynamic encryption, Dynamic coding table.

1.Introduction

In the past years, due to the proliferation of digital data and its ease of dealing, detection, sharing and reuse, many researchers have invented to work on techniques to increase the security of the transfer of this data and confidentiality, cryptography and Steganography are still the most important techniques[1].

Cryptography is the conversion of plain text to an illegible cipher, Return of the text to its explicit state on the other side depends generally on the algorithm used and the key, where the symmetric algorithm used the same key in both encryption and decryption process, that key must transfer in a secure channel. the different keys named "public and private" are used in asymmetric algorithm that depends on different keys in encryption and decryption process[2].

The algorithms that encrypt data are a blocks cipher algorithms and stream cipher algorithm, Encrypted data can be transmitted in a private channel or public channel, but the key in the symmetrical algorithms must be transmitted by the private channel, unlike the asymmetric methods, one of the keys which is public and does not need to be secret[3] .

In all cases and algorithms the data still present but in an unreadable format, it makes them more vulnerable to the threat[4].

Steganography is an embedding of digital message with the digital data of the cover; the cover may be an image, audio, movie, etc. When hiding in the image as in the proposed method there will be a stego-image. In general, the steganography in the image either in the temporal domain or in the transform domain. There are several techniques for hiding in both domains. Some types of steganography technique use the key and others do not use it, and is mostly used for more robust [5].

During the transfer process, the channel may be monitor intentionally or unintentionally, there are many hackers who wish to reveal the hidden data for different purposes. Therefore, the cover should be preserved with least possible changes. This means that there is a great similarity between the cover and the stego-object, and Difficulty to retrieve the secret message from stego-object at worst case [6].

In this paper, we propose two phases to encrypted text. Firstly the plain text converted to binary depending on dynamic substitution table, then it encrypted by AES algorithm which the dynamic key is generated by corner points. In the end, the data is hidden in the least significant bit exception these corner points.

2. AES Encryption Algorithm

AES is a symmetric cryptography algorithm, It a block cipher algorithm[7]. The length of the cipher keys can be 128, 192, or 256 bits. Both encryption and decryption procedures perform several rounds, due to the size of input/cipher key blocks. Input data in AES is often represented as 4*4 bytes array and it is termed as ‘‘state”[8].Figure 1 shows the AES encrypting steps.

There are four main phases: Add Round Key, Shift Rows, Sub Bytes, and Mix Columns. These four phases are used in every round except first and the last ones. The first round has only Add Round Key, and the last round does not have Mix Columns. The initial key has to be expanded to execute different rounds. The main phases are briefly described below:[[9]

1. Add Round Key: This phase adds a cipher key to a state array by using bitwise Exclusive-OR (XOR).
2. Shift Rows: This phase is a conversion that operates on the rows of a state. Bytes of the state are shifted cyclically to the left and right. The first row remains untouched. The second, third, and fourth rows are shifted by one, two, and three, respectively.
3. Substitute Bytes: This function is nonlinear. It performs a byte-by-byte substitution of the blocks to produce a new byte value. A substitution-box (S-Box) implemented by either a Look-Up Table or Galois Field operation.
4. Mix Columns: is a matrix multiplication with fixed values.

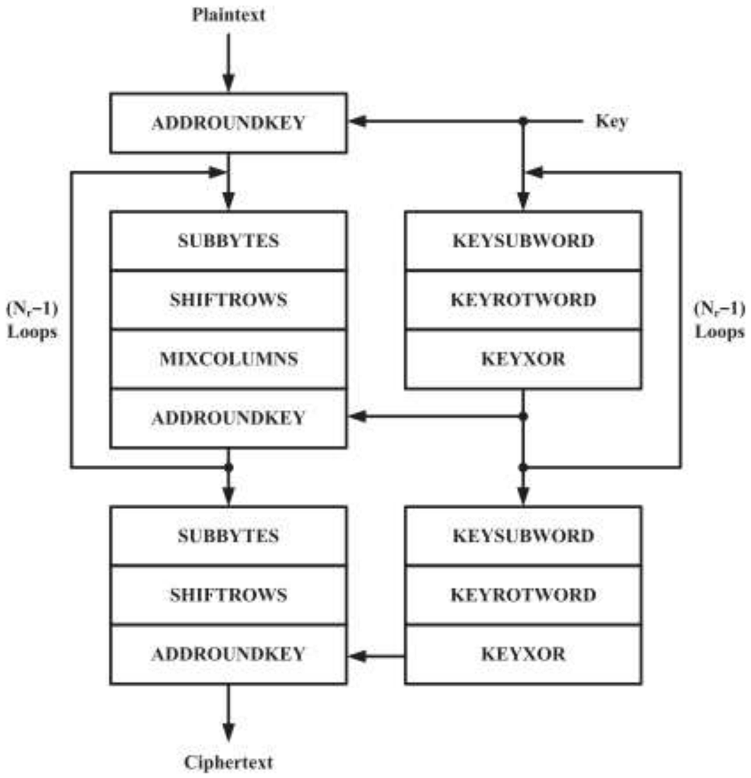


Figure 1. AES Encryption Steps [9]

3. Harris Corner Detection Algorithm

Harris algorithm is a still image algorithm used for the communal edge and edge detector. The amounts of corner functions are extracted that gives a better quantitative measurement that uses a steady operator. A local detection window is designed for it. With a minute shifting the window is shifted in diverse directions, and determined the average difference in intensity. As a corner point, the midpoint of the window is taken. By considering the intensity values in a minute window the point can be predicted. [10]

To identify the corner points, Harris algorithm uses corner detector. In a flat region will not show any difference of intensity in any directions in moving the window. It will show the difference in the edge direction if an edge section is found. But in a corner, there will be a considerable difference in intensity in every direction. The following shows the basic steps of Harris Corner Detection[11][12][13]

1. Compute x and y derivatives of image

   $I_x=G_\delta^x * I$ $I_y=G_\delta^y * I$

2. Compute products of derivatives of every pixel

   $I_{x2}=I_x.I_x$ $I_{y2}=I_y.I_y$

   $I_{xy}=I_x.I_y$

3. Compute the sums of the products of derivatives at each pixel

   $S_{x2}=G_{\delta 1}* I_{x2}$ $S_{y2}=G_{\delta 1}* I_{y2}$

   $S_{xy}=G_{\delta 1}*I_{xy}$

4. Define at each pixel (x,y) the matrix

   $$H(x,y)=\begin{vmatrix} S_{x2}(x,y) & S_{xy}(x,y) \\ S_{xy}(x,y) & S_{y2}(x,y) \end{vmatrix}$$

5. Compute the response of the detector at each pixel
   $R=Det(H)-K(\mathit{Trace}(H))^2$
6. Threshold on value of R. Compute nonMax suppression

4. Proposed method

In the proposed method two phases are done to encryption the text. First one is convert the plain text to binary code by dynamic substitution table which generated from cover image data. While the second phase is encrypted binary code using the AES algorithm depend on the dynamic key generate by using the Harris corner points .The hiding process for the encrypted code in the image has used the LSB of all image pixels excluding the pixels of corner points. The embedding and extracting processes shown in 'figure 2 'and 'figure 3'.

4.1 Proposed Algorithms

In this section, the algorithms of the proposed method are explained as shown below:

Algorithm 1: Data Embedding Algorithm

```
Input: plain text, cover image
Output: stego_ image
Step 1: generate dynamic coding table// generate 256 different bytes in coding table for
                                       256 characters that used in computer
i=0,                                  // i the counter of bytes in code table,
 j=0                                  // j the counter of bytes in cover image
while i<= 255 do
temp=   4 bits of MSB of byte[j] catenation with  4 bits of MSB of byte [j+1]
if temp not in code table
code table [char[i]]=temp
i=i+1
end if
  j=j+2
end while
step 2: convert the plain text to binary code by substitute character using the code table that
generated in step 1
step 3: apply Harris algorithm on cover image to  generate corner points.
Step 4:// generate dynamic 128 key for AES algorithm
i=1 ;                                   // i the counter of corner point bytes
key=0
  While i<= 32 do
Temp=(bit[0], bit[2], bit[4], bit[5]) from byte[i] of corner point array
     Key = key concatenation with Temp
i=i+1
End while
Step 5: apply AES algorithm on binary code that resultant from step2 using key from step 4 .
Step 6: hiding the encrypted data in LSB of the cover image exception the corner points.
```

Algorithm 2: Data Extracted Algorithm

```
Input: stego_image
Output: plain text
Step 1: generate the code table from the stego_image as in step 1 in algorithm 1.
Step 2: apply Harris algorithm on stego_image to get corner points.
Step 3: generate dynamic 128 bits key for AES algorithm depending on corner point as in step
4 in algorithm1
Step 4:  extract the encrypted text from the LSB of stego_image pixels except corner points.
```

Step 5: apply AES algorithm on extracted encrypted text using the128 bits key to get the binary code.
Step 6: generate plain text characters by substitute the binary code using the coding table.

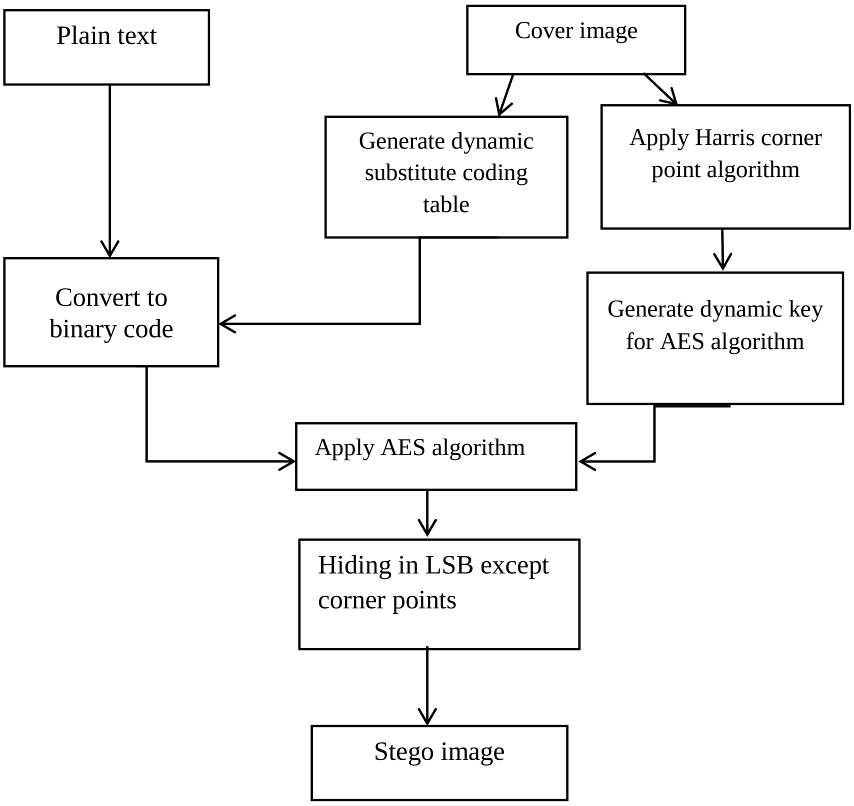

Plain text
Cover image
Generate dynamic substitute coding table
Apply Harris corner point algorithm
Convert to binary code
Generate dynamic key for AES algorithm
Apply AES algorithm
Hiding in LSB except corner points
Stego image

Figure 2. the embedding process

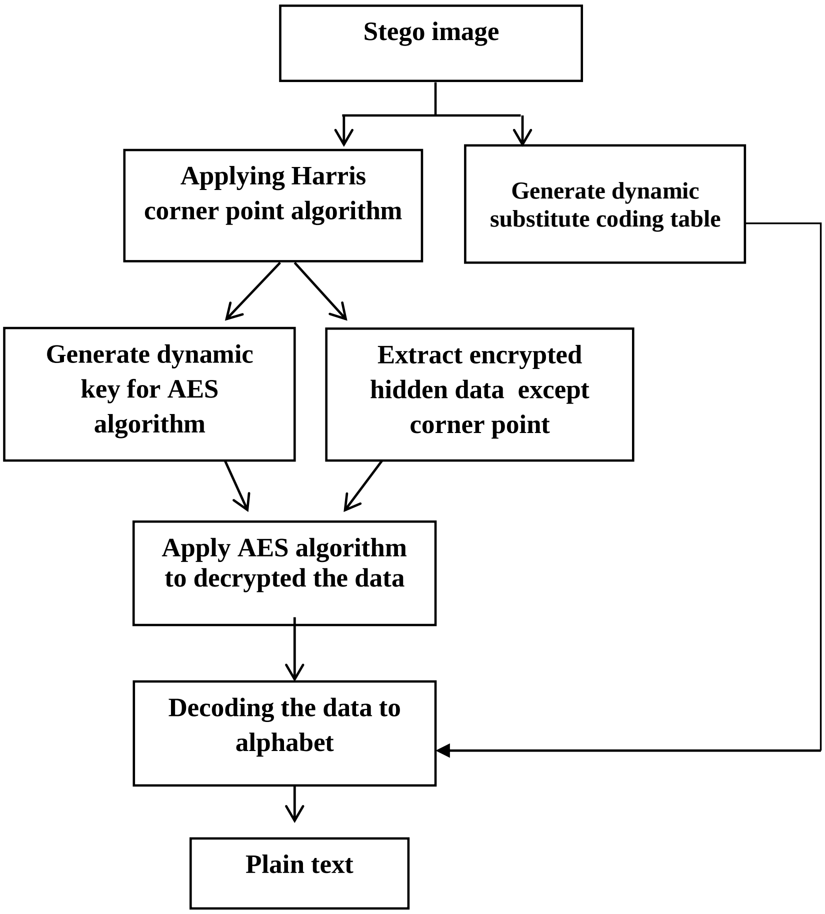

Stego image
Applying Harris corner point algorithm
Generate dynamic substitute coding table
Generate dynamic key for AES algorithm
Extract encrypted hidden data except corner point
Apply AES algorithm to decrypted the data
Decoding the data to alphabet
Plain text

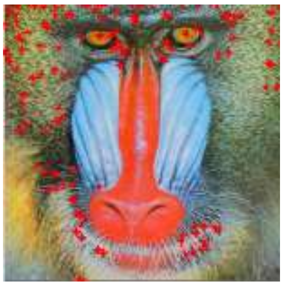
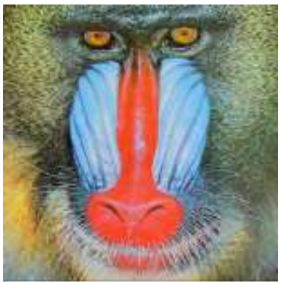
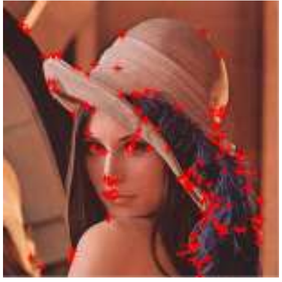
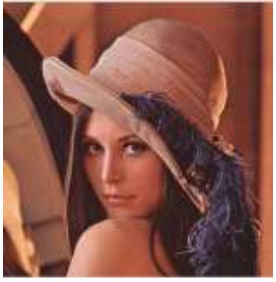
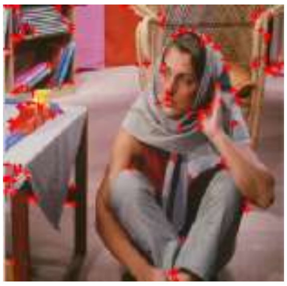
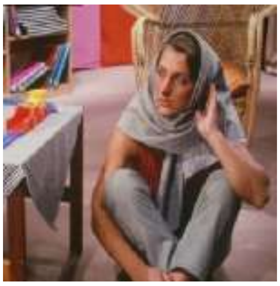
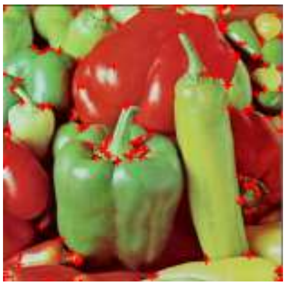
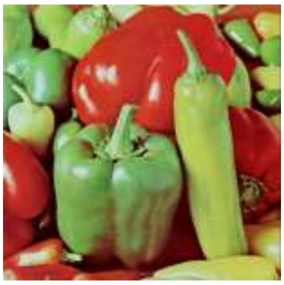
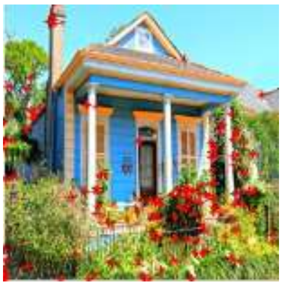
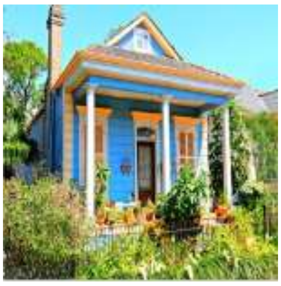
Figure 3. the extracting process

5.Experimental Results and Analysis

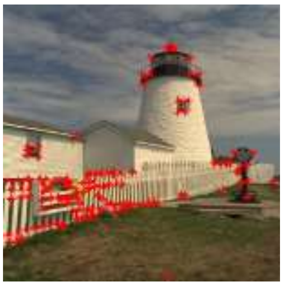
The proposed algorithm performed on many images with size 256x256x3, and 70 characters' message. The substitution table size is 256 records generated from the cover image, each record have two fields first to chars and the second to the binary coding. The corner points that generate from Harris algorithm are used to generate a dynamic key for the AES. The first, third, fifth, and sixth bits of each bytes of corner points were used until the end of the 128-bits key. this configuration is to increase the randomness of the key.

table (1) shows the cover image, the image with corner point and the result stego-image of six images as a samples for implement the proposed algorithm to compute the result. we can use image size more than 256*256 that give more load to hide with best result.

Table (1) the cover images, the images with corner points, and the stego-images

Image name	Cover image	image with corner point	stego-image
Baboon image			
Lena image			
Barbra image			
Pepper image			
House image			

Light house image



To evaluate the performance of proposed algorithm used parameters such as PSNR and MSE where

$$\mathrm{MSE} = \frac{1}{w \times h} \sum_{i=1}^{w} \sum_{j}^{h} \left(Stego\,(i,j) - Cover\,(i,j) \right)^2 \qquad \text{---------} \ (1)$$

Where, the Stego(i,j) is the stego_ image and the Cover(I,j) is cover image.

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255^2}{\mathrm{MSE}} \ (\mathrm{dB}) \qquad \text{---------} \ (2)$$

The proposed method does not need to exchange any information except cover-image and all information extract from cover-image until the secret message is retrieve , although it does not use the standard coding table and its using a symmetric encryption method that needs to exchange the key before the start of the encryption process.

The cryptographic flaws showed that the encryption text was larger than the original text (as result of standard AES algorithm, although that the proposed algorithm shows good average of PSNR as show in table(2).

Table (2) value of PSNR, and MSE for the proposed algorithm.

Image	PSNR	MSE
Baboon	80.9384	5.2389e-04
Lena	81.0668	5.0863e-04
Barbra	80.8138	5.3914e-04
Pepper	80.385	5.9509e-04
House	80.6163	5.6458e-04
Lighthouse	81.0668	5.0863e-04

6.Conclusion

In this work an efficient method for encryption and hiding is produce. The two phases in encryption process (dynamic substitution table and AES algorithm with dynamic key) are providing more security. To overcome the problem of exchange the key, the two parties generated it dynamically from image. The method of embedding data has used the most common and simplest way is the LSB of image pixels except the corner points extracted from the Harris algorithm. Although the cryptographic flaws showed that the encryption text was larger than the original text, the proposed method shows high value of PSNR. Also can used two or three LSB in each byte for hiding to increase the capacity of hiding data in cover image with good value of PSNR.

Reference

[1] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. **78**, no. December 2015, pp. 617–624, 2016.

[2] S. Sherkhane, A. Waghmare, S. Dalvi, and S. Bamne, "Hybrid Data Encryption using Color code and Armstrong number," vol. **7**, no. 4, pp. 10300–10305, 2017.

[3] S. Wade, A. Gadikar, A. Khan, and V. Deshmukh, "Design Enhance AES Data Encryption and Decryption," vol. **3**, no. 2, pp. 136–138, 2017.

[4] P. Dusane, J. Patil, U. Jain, R. Pandya, C. Engineering, and S. Coet, "Security of Data with RGB Color and AES Encryption Techniques," pp. 3063–3067, 2017.

[5] A. Judice, P. Shamini, D. J. Sree, and H. A. Sree, "An Image High Capacity Steganographic Methods by Modified OPA Algorithm and Haar Wavelet Transform," vol. **14**, no. 3, pp. 125–132, 2014.

[6] A. A. Abdul Latef and F. A. Abdul Latef, "Hiding Encrypted Color Image within MPEG-2 Video," vol. **30**, no. 4, pp. 605–614, 2012.

[7] N. Mathur and R. Bansode, "AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection," *Procedia Comput. Sci.*, vol. **79**, pp. 1036–1043, 2016.

[8] U. Farooq and M. F. Aslam, "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. **29**, no. 3, pp. 295–302, 2017.

[9] K. Shahbazi, M. Eshghi, and R. Faghih Mirzaee, "Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5," *Eng. Sci. Technol. an Int. J.*, 2017.

[10] M. Zhu, W. Wang, B. Liu, and J. Huang, "A Fast Image Stitching Algorithm via Multiple-Constraint Corner Matching," *Math. Probl. Eng.*, vol. 2013, 2013.

[11] P. V. Patil and M. S. C. Chavan, "A Comparative Analysis of Image Stitching Algorithms Using Harris Corner Detection And SIFT Algorithm .," vol. **10**, no. 1, pp. 482–486, 2017.

[12] Mahesh and M. . Subramanyam, "INVARIANT CORNER DETECTION USING STEERABLE FILTERS AND HARRIS ALGORITHM," *Int. J.*, vol. **3**, no. 4, pp. 1638–1645, 2011.

[13] Z. Zhang, H. Lu, X. Li, W. Li, and W. Yuan, "Application of Improved Harris Algorithm in Sub-Pixel Feature Point Extraction," *Int. J. Comput. Electr. Eng.*, vol. **6**, no. 2, pp. 101–104, 2014.