# Increase Security of Image Encryption Depends on Change Pixel Location

**Prof. Dr.Ziad M. Abood Zainab M.Essa**

Al-Mustansriyh University- College of Education

## Abstract

In any communication, security is the most important issue in today's world. The information security has be come one of the most signify can tproblemsin data communication. Lots of datasecurity and data hiding algorithmshavebeendevelopedinthelastdecade. Cryptography and steganography are the two major techniques for secret communication. In this paper, the secret text is first encryptedbyusingAESwhichhasverygood performanceandisamostpowerfultechnique. Now this encrypted text is embedded using steganography. Our proposed system gives threestages of security for secret. The main aim of proposed method to increase security of embedding and extraction phase using AESencryption,steganography and change pixel location. In order to evaluate performance the proposed algorithm performs series of tests. These tests include, PSNR and MSE.

**Keywords**: Cryptography, Steganography, AES.

## 1- Introduction

Since the beginnings of human information transfer, the wish to communicate in secrecy has existed. Whether planning a surprise birthday party or overthrowing a government, exchanging information in secret is essential. There has been multi solutions to this problem, the most usually used and investigated being "cryptography".[1]Historically, sensitive data has been protected using encryption. Encryption uses powerful mathematics to convert plaintext into an unreadable cipher text that is transmitting over a channel to the recipient. [2]When a message is encrypted it is done so using a "secret key". To decrypt a message, the secret key is used to reverse the operation. For an ease dropper to defeat the system he or she must get the secret key. Typically it is supposed that this must be done by searching through the entire key space; a so called "brute-force" attack. As this is a very time consuming endeavor, the "encrypted message" is considered safe[1][3].Second method of information transfer, called "steganography" offers information protection in a somewhat multiple manner. Steganography offers security like to cryptography in that, if an adversary does not know information is being transferred; he cannot intercept and read it. Though keeping the insides of a message secret is required in many cases, steganography have a much more powerful use steganography hides the very fact that a communication is taking place. The difference between cryptography and steganography is an important issue, and is summarized via the following: “Encryption prevents an unauthorized party from discovering the contents of a communication. Steganography prevents discovery of the very existence of a communication”. [4][5]

## 2-AES Algorithm

AES is a “symmetric block cipher” with length ofblock (128) bits and stand up for key lengths of (128, 192 and 256) bits. Evaluation criteria involve“security, flexibility, memory requirements, hardware and software convenient, and computational efficiency”. Table (1) shows key sizes and number of rounds. [6][7]

**Table (1) Key sizes versus rounds**

| Key Sizes Versus Rounds | | | |
|---|---|---|---|
| **Key lengths** | **Key Block size (Nk words)** | **Plaintext Block size (Nb words)** | **Number of Rounds (Nr)** |
| **AES-128** | **4** | **4** | **10** |
| **AES-192** | **6** | **4** | **12** |
| **AES-256** | **8** | **4** | **14** |

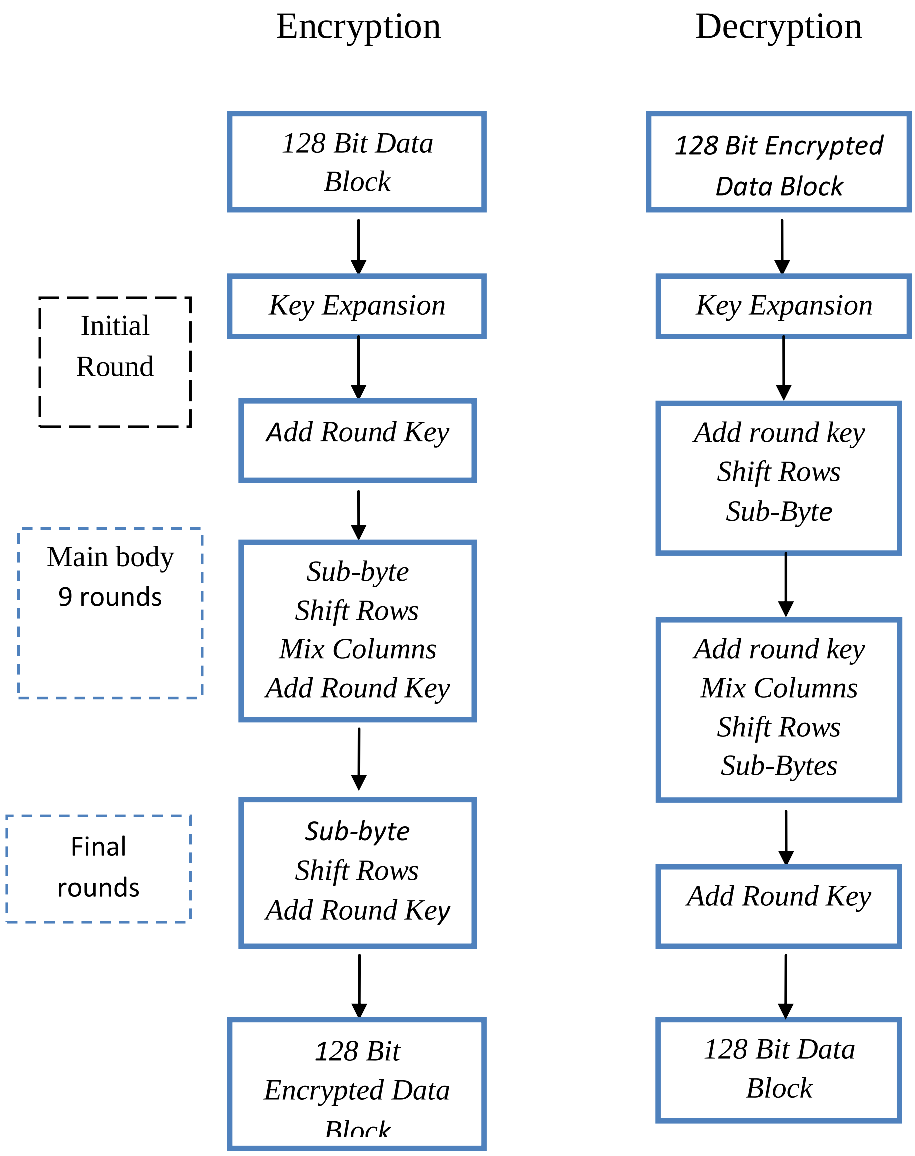
Encryption
Decryption
128 Bit Data Block
Key Expansion
Add Round Key
Sub-byte Shift Rows Mix Columns Add Round Key
Sub-byte Shift Rows Add Round Key
128 Bit Encrypted Data Block
Initial Round
Main body 9 rounds
Final rounds
128 Bit Encrypted Data Block
Key Expansion
Add round key Shift Rows Sub-Byte
Add round key Mix Columns Shift Rows Sub-Bytes
Add Round Key
128 Bit Data Block

**Fig.1 Steps of encryption and decryption**

## Steganography with Images

The "stego-image" is last product after secret message is inserted in "cover object". Secret message will be hidden in a "cover-image" by applying an inserted algorithm to create a "stego-image". The transfer of the "stego-image" via a communication channel is implemented via a sender to a receiver. [8] To show up the covert message that is hidden via the sender, the receiver wants to have the de-stego algorithm which is parameterized via a "stego-key" to abstract the secret message. That is the purpose of a "steganographic" system where an attacker who does not holding the "stego-key" or the name of fileto accessing it absolutely will not be capable to decide whether the file is even present. [9][10]In an effectual “steganographicsystem”, a typical cover medium should not be distinguishable from a stegoobject.“Steganography Mechanism Digital images”hasbe commonplace and nowhere are these images more prevalent than on the WWW in the Internet. The“digital images”use as a carrier medium is appropriate for hiding data because of their insensitivity for the human visual system(HVS). thatlarge numberfor web pages are impressively advanced with “color images” and thus Internet users browsing during the web no longer observe to sites having images or to the downloading of images and information files from the Web. Besides, there is a big number of plenty bits in an image. The plenty bits for an object are those bits that can be changed but the change cannot be visibly noticed via human eyes. [9]

## 3-The Proposed Method

This paper provides an overview of the proposed system, presenting the images used in this study and these images on different dimensions and with file format (BMP) and convert these images from RGB to Color model (HSV).

Figure(2) contains RGB images and HSV.

**#1** **#2** **#3**

**#4** **#5** **#6**

**Figure (2) RGB and HSV dataset images**

**Table (3) Cover images size and models**

| No.images | Sizeimages | Color model |
|---|---|---|
| #1- | 2718*1808 | RGB |
| #2- | 1280*1024 | RGB |
| #3- | 2560*1600 | RGB |
| #4- | 2718*1808 | HSV |
| #5- | 1280*1024 | HSV |
| #6- | 2560*1600 | HSV |

## 3-1 Diagram of proposed system

The proposed system consists of the technique that used encryption text, steganography and change pixel location by different methods and images quality calculation as shown in figure(2):

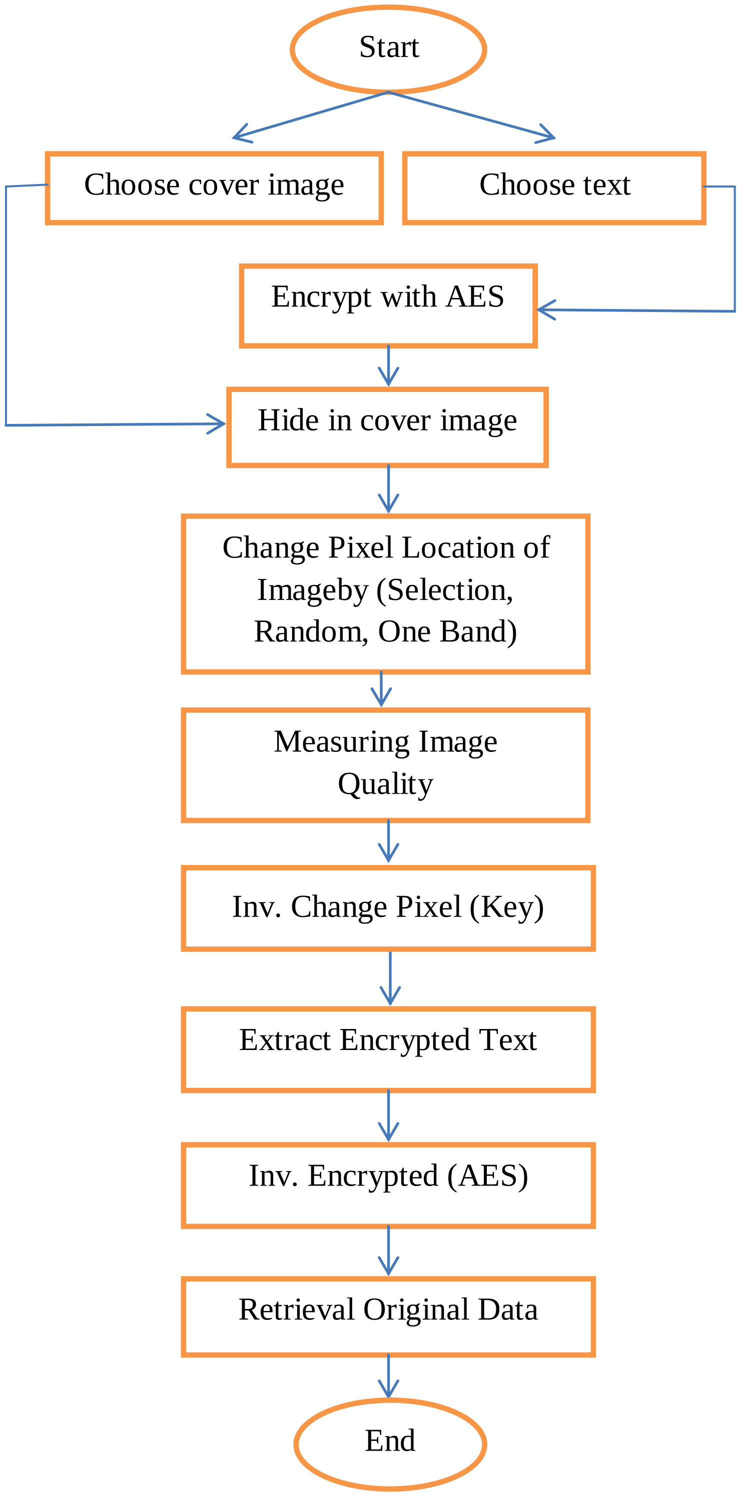

**Fig.3The proposed system**

## 4- Results and Discussions

It will be review the results that were obtained through the implement AES encryption method with LSB and change pixel location.The performance of the proposed approach has been studded usingtwo kinds of measures (PSNR, MSE). Shows in tables (4, 5, 6):

**Table (4) RGB, HSV selection change**

| Image no. | No. of pixel change | $PSNR_{RED}$ | $MSE_{RED}$ | Color model |
|---|---|---|---|---|
| #1- | 80 | 69.2319 | 0.0078 | RGB |
| #2- | 134 | 59.6212 | 0.0710 | RGB |
| #3- | 154 | 67.1625 | 0.0125 | RGB |
| #4- | 100 | 69.5649 | 0.0072 | HSV |
| #5- | 258 | 58.4172 | 0.0936 | HSV |
| #6- | 356 | 67.1827 | 0.0124 | HSV |

**Table (5) RGB, HSV random change**

| Image no. | No. of pixel change | $PSNR_{RED}$ | $MSE_{RED}$ | Color model |
|---|---|---|---|---|
| #1- | 130 | 60.8544 | 0.0534 | RGB |
| #2- | 400 | 51.4310 | 0.4677 | RGB |
| #3- | 600 | 53.9956 | 0.2591 | RGB |
| #4- | 200 | 56.3986 | 0.1490 | HSV |
| #5- | 450 | 48.7627 | 0.8646 | HSV |
| #6- | 700 | 52.2939 | 0.3834 | HSV |

**Table (6) RGB, HSV one band change**

| Image no. | No. of pixel change and the band | PSNR | MSE | Color model |
|---|---|---|---|---|
| #1- | 150 R | 99 | 0.1818 R | RGB |
| #2- | 300 B | 99 | 2.0636 B | RGB |
| #3- | 500 G | 99 | 0.5294 G | RGB |
| #4- | 200 R | 99 | 0.3971 R | HSV |
| #5- | 400 B | 99 | 1.6792 B | HSV |
| #6- | 800 G | 99 | 0.8535 G | HSV |

We observed that PSNR of the tested images using the proposedone band change has maximum value (99 dB) . MSE of the tested images using the proposed selection change has minimum value (0.0072).

## Conclusions:

This paper presented a description of increase security. The algorithm is employed effectively over an insecure channel and working against attacks by producing high imperceptible stego-images. Apply advanced encryption standard (AES) give better result with change pixel (random, selection, one band) depended on measurement results

(PSNR and MSE).AES encrypts different size of texts that contains numbers, letters and special character. In addition, LSB method is used for hiding encrypted data in cover images with models (RGB and HSV), format (BMP).

**References**

[1]IkhlasFalihAlsudany,"Analysis and Detection of Information Hiding in Digital Images", M.Sc, University of *Technology*, 2006.

[2] Neenu Daniel, Lini Abraham, An improved Color Image Encryption Algorithm with Pixel Permutation and Bit Substitution, IJRET: International Journal of Research in Engineering and Technology Volume: 02 Issue: 11, Nov-2013.

[3] Mohammad Ali, AmanJantan, Image Encryption Using Block-Based Transformation Algorithm, IAENG International Journal of Computer Science, 2008.

[4] AnupamMondal and ShiladityaPujari, A Novel Approach of Image Based Steganography Using Pseudorandom Sequence Generator Function and DCT Coefficients, Computer Network and Information Security, 2015.

[5] PrajaktaJagtap, Atharva Joshi, ShamsundarVyas, Reversible Data Hiding in Encrypted Images,International Advanced Research Journal in Science, Engineering and Technology, Vol. 2, Issue 2, February 2015.

[6] William Stallings,"Network Security Essentials",4th Ed,Prentice Hall 2011.

[7] Anup. Gujar, Image Encryption using AES Algorithm based on FPGA, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014.

[8] Pritha Roy and AsokeNath, New Steganography approach using encrypted secret message inside Audio and Video media, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 12, December 2014.

[9] G. Viji and J. Balamurugan,LSB Steganography in Color and Grayscale Images without using the Transformation,Bonfring International Journal of Advances in Image Processing,2011.

[10] C. P.Sumathi1, T. Santanam and G. Umamaheswari, A Study of Various Steganographic Techniques Used for Information Hiding, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

# زيادة الامن لصورة تحتوي بيانات مشفرة اعتمادا على موقع البكسل

**الخلاصة:**

في اي تبادل معلومات, والأمن هو أهم قضية في العالم اليوم.أصبح أمن المعلومات واحدة من أهم المشاكل في نقل البيانات.وقد وضعت الكثير من أمن البيانات و الخوارزميات لاخفاء البيانات في العقد الماضي. التشفير وإخفاء المعلومات نوعان من التقنيات الرئيسية للاتصال السري. في هذه الورقة، يتم تشفير النص السري لأول مرة باستخدام AES التي لديها الأداء الجيد جدا وتقنية أقوى.الآن هذا النص المشفريخفى باستخدام إخفاء المعلومات. النظام المقترح لدينا يعطي ثلاث مراحل للأمن. والهدف الرئيسي من الطريقة المقترحة لزيادة الأمن من تضمين ومرحلة استخراج باستخدام التشفير AES, إخفاء المعلومات وتغيير بكسل الموقع. من أجل تقييم أداء الخوارزمية المقترحة ينفذ سلسلة من الاختبارات. وتشمل هذه الاختبارات، PSNR و MSE.