MINAR International Journal of Applied Sciences and Technology

Article type : Research Article

Date Received :11/07/2021
Date Accepted : 08/08/2021
Date published : 01/09/2021
: www.minarjournal.com
http://dx.doi.org/10.47832/2717-8234.3-3.5

MSB BASED IMAGE STEGANOGRAPHY USING MCELIECE CRYPTOSYSTEM

Hayder Abdulkudhur MOHAMMED[1] & Najlae Falah Hameed Al SAFFAR[2]

Abstract

Steganography is the science of embedding secret data inside data so they can be sent to destination security. Encryption algorithms used to save information from sly activities when sent from one device to another over the wireless network. In this paper McEliece will be used to text encryption by Goppa code, where McEliece cryptosystem is a public-key cryptosystem based on error-correcting codes; then embedding the ciphertext as steganography image by MSB method. This lead to save information from attackers.

Keywords: Image steganography, Encryption, McEliece, MSB, and Goppa code.

[1] Kufa University, Iraq, haidera.algelahawi@student.uokufa.edu.iq, https://orcid.org/0000-0002-5370-7662

[2] Kufa University, Iraq, najlaa.hameed@uokufa.edu.iq, https://orcid.org/0000-0001-5599-2885

1. Introduction

Wireless networks are used in communication systems, where they enable more than two users to communicate without physical connections. Computer data are sent from the device to another across an insecure channel. This channel may be exposed to theft the data or modified. For this reason require protection of the data transmitted through insecure channels [1]. Cryptography converts messages into an unreadable form through the use of encryption algorithms. The cryptography is concerned with several objectives confidentiality, integrity, availability, and authentication [2]. Cryptography is used to guarantee the secrecy and the authenticity of information by different techniques and algorithms. steganography has an important role in secret communication. McEliece proposed an alternative to such systems in 1978 [3]. It consists in a public-key cryptosystem based on error-correcting codes. Together with its Niederreiter version - of equivalent security - the original system based on the family of Goppa codes still resists cryptanalysis. The general security of the scheme relies on the inherent intractability of decoding a random code up to its error-correcting capability. The great advantage of systems based on error-correcting codes is the extremely low cost of their encryption and decryption procedures [4].Steganographic processes can be classified into two categories: spatial and transform domains approaches [5]. Used digital images for steganography [6]; Image steganography techniques require two files: cover image, and the data (message) to be secretly hidden [7]. Steganography and cryptography are the procedures for making certain about the cataloguing and anonymous information. The anonymous data that is to be taken from the developers is a tough task. Steganography obscures existence of the information and safeguard anonymous information from an unapproved get to. The information hiding structure encompasses the following subcomponents: the important message to be stored, an original image in which to store the data, and the resulted hidden image or text [8]. The technique for hiding essential information using most significant bits (MSB) of image pixels has presented. The number 8 an is calculated secret data bit. Then, value of bit number 8 is altered. The consequences generated from the above investigation reveals that the projected method advances signal to noise ratio. The paper assesses several methods and techniques used in stegano scrutiny, notions and techniques used in spatial representation [9]. Tiwari et al. in 2015 introduced a new method for concealing messages in a color image based on chaos theory, which used two chaotic logistic maps one for choosing the position of pixels randomly and the other for inserting the message's bits. This method is robust and the higher payload capacity [10].Recommends a new technique for image encoding by loading the data with the carefully chosen pixel and on the subsequent value of the given pixel. A log is entered and the specified pixel is used to collect the base bit of the data and the pixel value is replaced with 0 or 1 to store another bit of data. By applying the most significant bit function to 8 bits of image data.[11].

2. McEliece Cryptosystem

In cryptography, the McEliece cryptosystem is an asymmetric encryption algorithm developed in 1978 by Robert McEliece[3]. It was the first such scheme to use randomization in the encryption process. The algorithm is based on the hardness of decoding a general linear code [12]. For a description of the private key, an error-correcting code is selected for which an efficient decoding algorithm is known, and which is able to correct t errors. The original algorithm uses binary Goppa codes (subfield codes of geometric Goppa codes of a genus-0 curve over finite fields of characteristic 2); these codes can be efficiently decoded, thanks to an algorithm due to Patterson[13]. The public key is derived from the private key by disguising the selected code as a general linear code. For this, the code's generator matrix G is perturbated by two randomly selected invertible matrices S and P.McEliece consists of three algorithms: a probabilistic key generation algorithm which produces a public and a private key, a probabilistic encryption algorithm, and a deterministic decryption algorithm.

Key Generation Algorithm

The principle is linear code C from some family of codes for which knows an efficient decoding algorithm, this choice should give rise to an efficient decoding algorithm A, and to make C public knowledge but keep the decoding algorithm secret. The steps are as follows:

1. Alice selects a binary (n, k)-linear code, C capable of (efficiently) correcting, t errors from some large family of codes, G be any generator matrix for C.
2. Alice selects a random k* k binary non-singular matrix S.

3. Alice selects a random n* n permutation matrix P.
4. Alice computes the k* n matrix G'=SGP, where G' is an encoding matrix.
5. Alice's public key is (G', t); her private key is (S,P,A). Note that A could be encoded and stored as the parameters used for selecting C.

Message Encryption Algorithm

Suppose Bob wishes to send a message m to Alice whose public key is (G',t):

1. Bob encodes the message m as a binary string of length k.
2. Bob computes the vector C'=m*G'.
3. Bob generates a random n-bit vector z containing exactly t ones a vector of length n and weight t.
4. Bob computes the cipher text as C=C'+z.

Message Decryption Algorithm

Upon receipt of c, Alice performs the following steps to decrypt the message:

1. Alice computes the inverse of P .
2. Alice computes C'=C*P-1.
3. Alice uses the decoding algorithm A to decode C' to m'.
4. Alice computes m=m'*S-1

1.2 Goppa Codes

Born in 1939, a Soviet and Valery Denisovich Goppa (a Russian mathematician) discovered the relation between algebraic geometry and codes in 1970. This led to the idea of Goppa Codes. It turned out that Goppa codes also form arguably the most interesting subclass of alternant codes, introduced by H. J. Helgert in 1974. These codes have got efficient decoding algorithm by N. Patterson [13] in 1975.

The explanation comes with this example: CalculatingGoppa matrix of $\mathrm{g(x) = x^2 + a^7x + 1}$, on $\mathrm{GF(2^4)}$ under module primitive polynomial $\mathrm{m(x) = x^4 + x + 1}$, as follows:

$\mathrm{m = 4,\ p = 2, t = 2, n = 12}$, the dimension k of $\mathrm{r(L_{,}\ g(x)}$) be at least $k \geq n - mt = 12 -\ 2 \cdot 4 = 4$, and the minimum distance of the code satisfied $d \geq t\ + 1 = 2 + 1 = 3$. The representation of elements of GF (2^4) as the powers of a, where $\mathrm{a = \alpha}$, using $\mathrm{a^4 = a + 1}$.

	0	$(0000)^T$	a^7	$a^3 + a + 1$	$(1101)^T$
-	1	$(1000)^T$	a^8	$a^2 + 1$	$(1010)^T$
a	a	$(0100)^T$	a^9	$a^3 + a$	$(0101)^T$
a^2	a^2	$(0010)^T$	a^{10}	$a^2 + a + 1$	$(1110)^T$
a^3	a^3	$(0001)^T$	a^{11}	$a^3 + a^2 + a$	$(0111)^T$
a^4	$a + 1$	$(1100)^T$	a^{12}	$a^3 + a^2 + a + 1$	$(1111)^T$
a^5	$a^2 + a$	$(0110)^T$	a^{13}	$a^3 + a^2 + 1$	$(1011)^T$
a^6	$a^3 + a^2$	$(0011)^T$	a^{14}	$a^3 + 1$	$(1001)^T$

To find the parity check matrix H, we can use the formula of previous page, and $\mathrm{g(x)} = \mathrm{x}^2 + \mathrm{a}^7\mathrm{x} + 1$, then $\mathrm{g}_1 = \mathrm{a}^7, \mathrm{g}_2 = 1$, and since L={$\mathrm{a}^{\mathrm{i}} \mid 2 \le \mathrm{i} \le 13$}, $\mathrm{a}_1 = \mathrm{a}^2$, $\mathrm{a}_2 = \mathrm{a}^3, \dots, \mathrm{a}_{12} = \mathrm{a}^{13}$, the factors $\mathrm{h}_{\mathrm{i}} = \mathrm{g}(\mathrm{a}_{\mathrm{i}})^{-1}$ are computed for $1 \le \mathrm{i} \le 12$.

$$\begin{aligned}
h_1 &= g(a^2)^{-1} = (a^4 + a^9 + 1)^{-1} = ((1100)^{\mathrm{T}} + (0101)^{\mathrm{T}} + (1000)^{\mathrm{T}})^{-1} = (10001)^{\mathrm{T}})^{-1} \\
&= (a^3)^{-1} = a^{12} \\
h_2 &= g(\alpha^3)^{-1} = (a^6 + a^{10} + 1)^{-1} = ((0011)^T + (1110)^T + (1000)^{\mathrm{T}})^{-1} \\
&= ((0101)^T)^{-1} = (a^9)^{-1} = a^5 \\
h_3 &= g(\alpha^4)^{-1} = (a^8 + a^{11} + 1)^1 = ((1010)^{\mathrm{T}} + (0111)^T + (1000)^{\mathrm{T}})^{-1} = ((0101)')^{-1} \\
&= (\alpha^9)^{-1} = \alpha^6 \\
h_4 &= g(\alpha^5)^1 = (\alpha^{10} + a^{12} + 1)^{-1} = ((1110)^{\mathrm{T}} + (1111)^T + (1000)^T)^{-1} = ((1001)^T)^{-1} \\
&= (\alpha^{14})^{-1} = a \\
h_5 &= g(\alpha^6\}^{-1} = (a^{12} + a^{13} + 1)^1 = ((1111)^T + (1011)^T + (1000)^{\mathrm{T}})^{-1} \\
&= ((1100)^{-1} = (\alpha^4)^{-1} = a^{11} \\
h_6 &= g(a^7)^{-1} = (a^{14} + a^{14} + 1)^{-1} = (1)^{-1} = ((1000)^T)^{-1} = 1 \\
h_7 &= g(\alpha^8)]^{-1} = (\alpha^{16} + a^{15} + 1)^{-1} = (\alpha + 1 + 1)^{-1} = (a)^{-1} = a^{14}, \\
h_8 &= g(\alpha^9)\}^{-1} = (a^{18} + a^{16} + 1)^{-1} = (a^3 + a + 1)^{-1} = (a^7)^{-1} = a^8 \\
h_9 &= g(a^{10})^{-1} = (\alpha^{20} + a^{17} + 1)^{-1} = (a^5 + a^2 + 1)^{-1} = ((1100)^T)^{-1} = (\alpha^4)^{-1} = a^{11} \\
h_{10} &= g(\alpha^{11})^1 = (a^{22} + a^{18} + 1)^1 = (a^7 + a^3 + 1)^{-1} = ((0100)^T)^1 = (a)^{-1} = a^{14} \\
h_{11} &= g(\alpha^{12})^{-1} = (a^{24} + a^{19} + 1)^{-1} = (a^9 + a^4 + 1)^{-1} = ((0001)^T)^{-1} = (a^3)^{-1} = a^{12} \\
h_{12} &= g(\alpha^{13})^{-1} = (a^{26} + a^{20} + 1)^{-1} = (a^{11} + a^5 + 1)^{-1} = ((1001)^T +^{-1} = (a^{14})^{-1} = a
\end{aligned}$$

$$H = \begin{pmatrix} (g_1 + g_2.a_1) \cdot h_1 & (g_1 + g_2.a_2) \cdot h_2 \dots (g_1 + g_2.a_2).h_{12} & \\ g_2 \cdot h_1 & g_2.h_2 & m_2 \cdot h_{12} \end{pmatrix}$$

$$H = \begin{pmatrix} (\alpha^7 + a^2), h_1 & (a^7 + a^3) \cdot h_2 & \dots & (a^7 + a^{13}), h_{12} \\ h_1 & h_2 & \dots & h_{12} \end{pmatrix}$$

$$H = \begin{pmatrix} a^9 & a^{10} & a^9 & a^{14} & a^6 & 0 & a^{10} & a^8 & a^2 & a^7 & a^{14} & a^6 \\ a^{12} & a^6 & a^6 & a & a^{11} & 1 & a^{14} & a^8 & a^{11} & a^{14} & a^{12} & a \end{pmatrix}$$

$$H = \begin{pmatrix}
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
- & - & - & - & - & - & - & - & - & - & - \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0
\end{pmatrix}$$

The generator matrix G can be computed from H by using $G\mathrm{H}^{\mathrm{T}} = 0$, so the vectors in the nullspace of H modulo 2 form the rowspace of G. In this case, G is as follow:

$$G = \begin{bmatrix}
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1
\end{bmatrix}$$

1. MSB of Image Steganography

In computing, the most significant bit (MSB, also called the high-order bit) is the bit position in a binary number having the greatest value. The MSB is sometimes referred to as the left-most bit due to the convention in positional notation of writing more significant digits. Further to the left. The MSB can also correspond to the sign of a signed binary number in one, Although a few CPU manufacturers assign bit numbers the opposite way (which is not the same as different endianness), the MSB unambiguously remain the most significant bit. This may be one of the reasons why the term MSB is often used instead of a bit number, although the primary reason is probably that different number representations use different numbers of bits. By extension, the most significant bits (plural) are the bits closest to, and including, the MSB[14].

Algorithm of MSB Based Steganography:

1. Convert image to pixels.
2.Converting pixels to 8-bit binary.
3. Change the value of the first bit.

2. Proposed Algorithm

Image cryptography is the process of transforming an image to ensure its security. Due to the rapid development of the Internet in today's digital world, the security of images has become more and more important. The security of digital images has recently received more attention, for which many different image encryption technologies have been introduced.

McEliece uses a public-key based on algebraic coding theory which makes use of a linear error-correcting code for which a fast decoding algorithm exists, namely a Goppa code.

2.1 Algorithm of embedding ciphertexted by McEliece in MSB Image

Input: An image and information (message).
Output: Steganography image.
Step 1: find key by Goppa code, where G matrix is key.
Step 2: encryption message by McEliece method.
Step 3: hiddencipher text in gray image by MSB.
Step 4: 16-bit for number of text, 16-bit for location select in image.
Step 5: result is steganography image.

2.2 Implementation of Proposed Algorithm

In this the example can be explained of proposed method as follows:

Plaintext: 'messag-by-McEliece22'
Key of Goppa code:

$$s = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$p = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$G = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

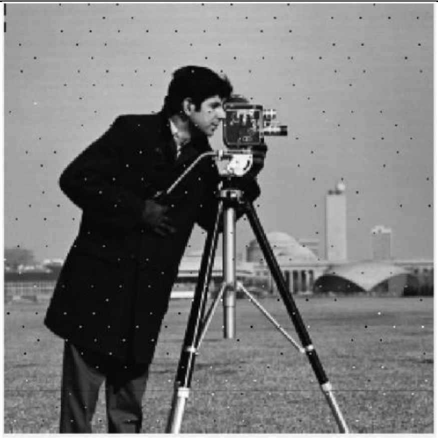
$$e = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0]$$

The ciphertext will be:
Ï-□ˆ(Çþ7IñJ`LÔ¡»Nð/× èSê¾»¼D^Aà4KGÛ>□vh□)‹qéLòÊ2□º• (all these symbols is coming after doing the encryption steps)

Steganography steps:

1- Select 32-bit to hidden information of text.
2- Select 16-bit to number of letters.
3- Select 16-bit to number of location select.
4- Hidden in location selected by shift, where shift= size image/ number of letters.

Table1: Implementation of the proposed method for Camerman$^{(256\times256)}$ image

Orignal image				Stego image			
							
154	156	165	162	26	156	165	162
107	128	128	114	235	0	128	242
155	158	163	163	155	30	163	35
89	136	109	159	89	136	109	159
Message= [0110 1001 1110 1101]							
10011010	10011100	10100101	10100010	00011010	10011100	10100101	10100011
01101011	10000000	10000000	01110010	11101011	00000000	10000000	11110010
10011011	10011110	10100011	10100011	10011011	00011111	10100011	00100011
01011001	10001000	01101101	10011111	01011001	10001001	01101100	10011110

3. Security Analysis

In this section explain some measures to find the resolution of the work:

3.1 Histogram Analysis

An image histogram is a gray-scale value distribution showing the frequency of occurrence of each gray-level value. For an image size of 1024 × 1024 × 8 bits, the abscissa ranges from 0 to 255; the total number of pixels is equal to 1024 × 1024. Modification of original histograms very often is used in image enhancement procedures.

As table 2, the result show that the histogram of the original image (gray and color types) and of the Image with hidden message almost same with uniform distribution, which means that the proposed algorithm recovers the image well, which is mean that is no useful information can be extracted from the encrypted image, and high security can be guaranteed to resist statistical attacks.

3.2 Pick Signal to noise ratio

Mean Square Error(MSE): it represents the quality of image has hiding data. Its equation is [15]:

$$MSE = \sum_{i=1}^{N}\sum_{j=1}^{M}(S(i,j) - I(i,j))^2 \Big/ M * N$$

Peak Signal-to-Noise Ratio (PSNR): is the ratio of the maximum signal to noise in the stegoimage. PSNR value if large indicates the better quality of the image while is was less alteration.Its equation is [15]:

$$PSNR = 10\,log10\,(\frac{MAX^2}{MSE})$$

According to table 2, the PSNR is constantly above 50 for color images, while is was less than 50 for grey image,, these results pointed that the hiding data hardly be perceived for color images, this is because of the fact that a high quality encrypted image should strive more than 40 as a value of PSNR.

3.3 Pearson Correlation Coefficient

Pearson correlation coefficient (PCC), is a statistical means that measures the direction and strength of a linear correlation between two random signals [16], in other words, PCC measures the linear dependence between two random signals. It is useful in various subjects in statistics, such as data classification [17], data analysis, clustering, the decision making [18], the finance analysis [19], and research of biology [20].

PCC of two signals $A$and $B$is accurately described as the covariance of the two signals divided by the product of their standard and it be described by [21]:

$$\mathrm{PCC} = \frac{\sum_{i=1}^{N}(A_i - \bar{A})\ \sum_{i=1}^{N}(B_i - \bar{B})}{\sqrt{\sum_{i=1}^{N}(A_i - \bar{A})^2}\ \sqrt{\sum_{i=1}^{N}(B_i - \bar{B})^2}}$$

Where $\bar{A} = \frac{\sum_{i=1}^{N} A_i}{N}$, $\bar{B} = \frac{\sum_{i=1}^{N} B_i}{N}$ and N is the signal length and $\bar{x}$ and $\bar{y}$ are the mean values of$x$ and y respectively, the coefficient PCC ranges from 0 to 1. The PCC gives a sign on the direct relation between the two arbitrary signals A and B. If the signals are directly related, the sign of the correlation coefficient is positive. If$PCC = 0$, A and B are said to be unrelated.

According to table 2, the PCC values for all implementations image are almost0.9999, this mean that the proposed algorithm is an efficient one.

Table 2: Implementation of proposed method for different images with results of measures of security analysis

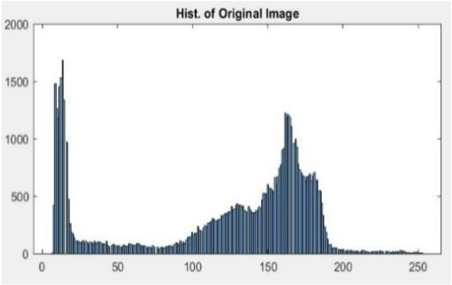
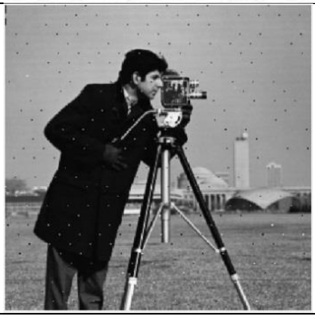
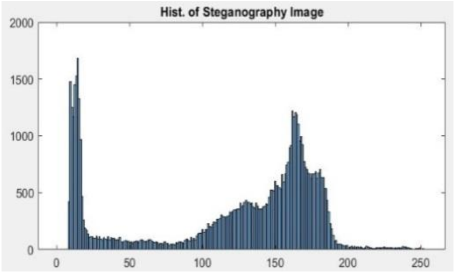
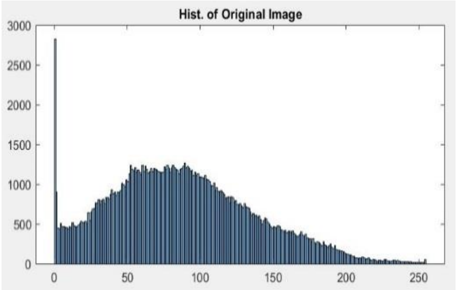
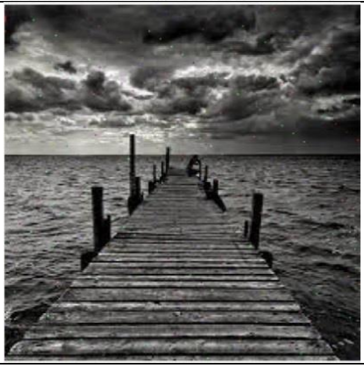
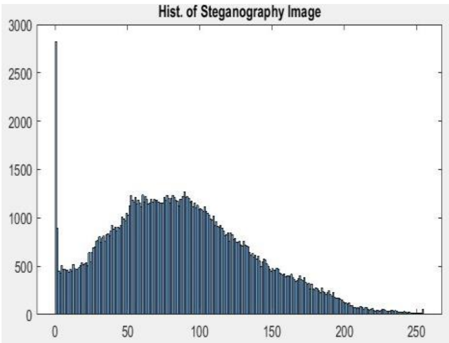
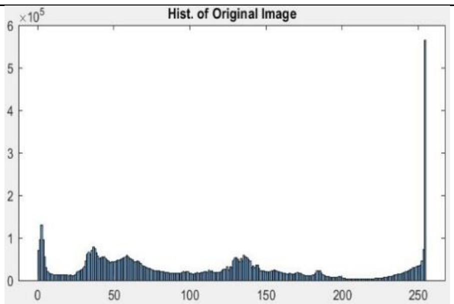
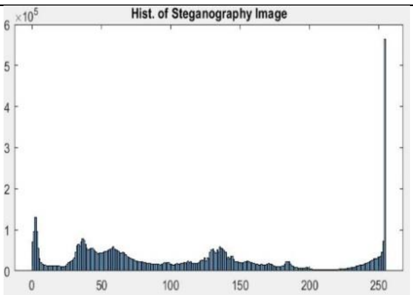
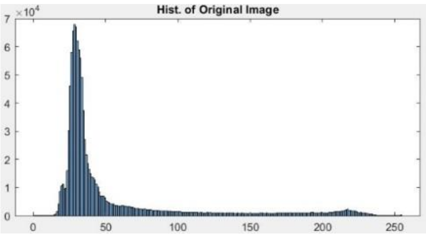
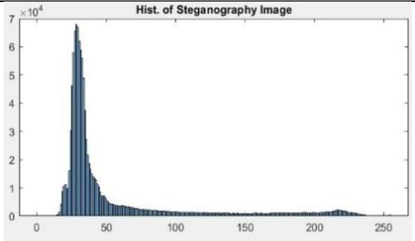
Images	Image	Histogram	MSE	PSNR	Correlation
Orignal Image			65.500	29.9683	0.9968
Image with hidden message					
Orignal Image			24.4883	34.2412	0.9987
Image with hidden message					
Orignal Image			0.5902	50.42064	0.9999

Image with hidden message					
Orignal Image			0.0002	84.8046	0.9999
Image with hidden message					

4. Conclusion

McEliece public key cryptosystem used in applications where long term security is needed. There are no known classical or quantum computer attacks on McEliece's cryptosystem which have sub-exponential running time. Despite the lack of efficient attacks on McEliece's proposal, none of the cryptographic schemes based on coding theory is proven to be as secure as some classic problem of coding theory. The text is encrypted using McEliece algorithm and embedded within an image using new technique gives more security to the proposed algorithm in general. This according to the result and histogram analysis, it is conclude that PSNR values for color images are more than the limit required to know the efficiency of the algorithm for color images.

5. References

Stinson. D. R.," Cryptography: Theory and Practice", printed in the United States of America, 2006.

Stallings William, "Cryptography and Network Security", Printed in the United States of America, 2014.

R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical report, Jet Propulsion Lab. DSN Progress Report, 1978.

Y. X. Li, R. H. Deng, and X. M. Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Transactions Information Theory, 40(1):271–273, 1994.

A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital imagesteganography: Survey and analysis of current methods", Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.

B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 2073-4212, 2011.

Khan Z, Shah M, Naeem M, Mahmood T, Khan SNA, et al. (2016) Threshold based Steganography: A Novel Technique for improved Payload and SNR " , International Arab J inform Technol 13: 380-386.

Bn L , Junhu H, wu Huang J, Qngsh Y (2017) A Survey on image Steganography and Steganalysis J Inform Hiding Multimedia Signal Process 2.

A. K. Tiwari, A. Rajpoot, K. K. Shukla, and S. Karthikeyan, "A Robust Method for Image Steganography based on Chaos Theory," International Journal of Computer Applications, vol. 113, No. 4, 2015.

Kadh m NJ, Premaratne P, Vial PJ, Halloran, B (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research Neurocomputing 335 : 299–326.

Robert J., "A Public-Key Cryptosystem Based on Algebraic Coding Theory" (PDF). DSN Progress Report, (1978).

N. J. Patterson . "The algebraic decoding of Goppa codes". IEEE Transactions on Information Theory, (1975).

Rohit Garg and Tarun Gulati (2012). Comparison of Lsb & Msb Based Steganography in Gray-Scale Images, International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 8

Zahraa Kadhim, Najlae Falah Hameed Al Saffar, “Image encryption based on elliptic curve cryptosystem”, International Journal of Electrical and Computer Engineering 11(2), pp. 1293-1302, 2021.

S. K. Tyagi, "Correlation coefficient of dual hesitant fuzzy sets and its applications," Applied mathematical modelling, vol. 39, no.22, pp. 7082-7092, 2015.

D. Pavanello, W. Zaaiman, A. Colli, J. Heiser, and S. Smith, "Statistical functions and relevant correlation coefficients of clearness index," Journal of Atmospheric and Solar-Terrestrial Physics, vol. 130, pp. 142-150, 2015.

H. Liao, Z. Xu, and X.-J. Zeng, "Novel correlation coefficients between hesitant fuzzy sets and their application in decision making," Knowledge-Based Systems, vol. 82, pp. 115-127, 2015.

Y. Kim, T.-H. Kim, and T. Ergün, "The instability of the Pearson correlation coefficient in the presence of coincidental outliers," Finance Research Letters, vol. 13, pp. 243-257, 2015.

J. Lee Rodgers and W. A. Nicewander, "Thirteen ways to look at the correlation coefficient," The American Statistician, vol. 42, no.1, pp. 59-66, 1988.

J. Ahmad and F. Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes," International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS, vol. 12, pp. 18-31, 2012.