A Modified Method of Information Hiding Based on Hybrid Encryption and Steganography

Baedaa H. Helal *

Received: 3/7/2011
Accepted: 22/11/2011

Abstract

This paper produces a developed method based on steganography techniques to prevent intruders from obtaining the transmitted information. This work is based on a combination of steganography and cryptography techniques to increase the level of security and to make the system more complex to be defeated by attackers. The algorithm used for encryption is the RC6 algorithm.

Two methods of hiding are used in this work: the first method is the Least Significant Bit (LSB) and the second is the proposed and modified method used to hide bits in LSB of iterated loop in brightness, red, green and blue of hiding image. The proposed method was tested using standard objective measures such as Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). A comparison between the two methods is performed.

Key word: steganography techniques, cryptography techniques, MATLAB program.

طريقة معدّلة لإخفاء المعلومات اعتمادا على ستراتيجية هجينة بين الاخفاء والتشفير

الخلاصة

البحث الحالي يقدم طريقة مطورة تعتمد على تقنية الاختزال لمنع الدخلاء من الحصول على المعلومات المرسلة , ذلك بالاعتماد على فن الاختزال وتقنية التشفير لغرض زيادة مستوى السرية وجعل النظام اكثر تعقيدا للحفاظ عليه من المهاجمين , الخوارزمية المستخدمة في التشفير هي خوارزمية RC6 .

في البحث الحالي تم استخدام طريقتين للاخفاء , الاولى هي the Least Significant Bit (LSB) والثانية هي طريقة مقترحة معدلة تستخدم اخفاء البايت في LSB بشكل حلقة متكررة في مناطق السطوع واللون الاحمر والاخضر والازرق في الصورة المستخدمة كغطاء . تم اختبار الطريقة المقترحة باستخدام الاجراءات القياسية المعتمدة مثل متوسط مربع الخطأ (MSE) ونسبة ذروة الاشارة الى الضوضاء (PSNR). واعتمادا على هذه المقاييس تم المقارنة بين اداء الطريقتين.

*Control and Systems Eng. Dept., University of Technology

This research is selected form the conference for publication in IJCCCE Journal

1. Introduction:

Digital communication has become an essential part of nowadays infrastructure. A lot of applications are Internet-based and in some cases it is desired that communication be made secret. Consequently, the security of information has become a fundamental issue. Many techniques are available to achieve this goal some of them are the Encryption and the steganography techniques. Using cryptography, the information is transformed into some other gibberish form and then the encrypted information is transmitted. Steganography is a process that involves hiding a message in an appropriate carrier for example an image or an audio file. Steganography can be applied electronically by taking a message (a binary file) and some sort of cover (often a sound or image file) and combining both to obtain a "stego-object"**.** The stego-object is essentially the cover with its redundant information replaced with the message. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message [1].

Steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Modern steganography is generally understood to deal with electronic media rather than physical objects and texts. This makes sense for a number of reasons. First of all, because the size of the information is generally (necessarily) quite small compared to the size of the data in which it must be hidden (the cover file), electronic media are much easier to manipulate in order to hide data and extract messages. Secondly, extraction itself can be automated when the data is electronic, since computers can efficiently manipulate the data and execute the algorithms necessary to retrieve the messages. Electronic data also often includes redundant, unnecessary, and unnoticed data spaces which can be manipulated in order to hide messages [2].

Previous attempts at achieving this goal have required the user to provide the original cover as well as the stego-object. The best areas to hide are first identified in the original cover, then these areas are mapped across to the stego-object and the hidden information is retrieved. The original cover must be provided because the information overwritten in the message hiding process may have been used to identify the best hiding areas. However, to provide the original object is not secure, because taking the differences between the two objects would be enough to suspect the existence of (and in some cases, recover) the hidden information.[3]**.**

2. Framework of Steganography Model:

In general, the basic framework of the steganography model is illustrated in Figure (1).

This model consists of two main processes, namely the Embedding process and the Extracting process. The main function of the embedding process is to hide the secret message, called Embedded message, in a given cover, called Cover-file. In hidden communication techniques, the cover-file is no more than an innocent (unrelated to the embedded message) piece of information that is used to hide the secret information. A secret key, called Stego-key is used in the embedding process so that it makes the embedded message computationally infeasible to extract without possessing this key. The output of the embedding process is called Stego-file, which is the original file holding the hidden secret message. This output becomes, at the other end, the input of the extracting process, in which the embedded message is extracted from the Stego-file to complete the hidden communication process. Since the stego-key is used in the embedding process, it needs to be used in the extracting process [4].

3. Cryptography

The process of encryption and decryption is called a ciphering as shown in figure (2). All modern algorithms use a key to control encryption and decryption; a message can be decrypted only if the key matches the encryption key.

Basically, the purpose of cryptography and steganography is to provide secret communication. Many people lump Steganography with cryptography, and while they are in many cases means to the same ends they are not the same thing.

Cryptography is the science of converting plaintext into ciphertext, which protects the contents of messages. [5], [6]

3.1-Details of RC6:

RC6 is a block cipher submitted to NIST for consideration as the Advanced Encryption Standard (AES). RC6 is a fully parameterized family of encryption algorithms. A version of RC6 is more accurately specified as RC6-w/r/b where the word size is w bits, the encryption consists of a nonnegative number of rounds r, and b denotes the length of the encryption key in bytes. [7]

RC6 works with four 32-bit registers A; B; C; D which contain the initial input plaintext as well as the output ciphertext at the end of the encryption. The first byte of plaintext or ciphertext is placed in the least-significant byte of A; the last byte of plaintext or ciphertext is placed into the most-significant byte of D. Use the (A; B; C; D) = (B; C; D;A) to mean the parallel assignment of values on the right to registers on the left, figure (3).

3.2- Least Significant Bit Embedding

It is one of the basic and easily implemented image steganography methods. This is done by embedding one bit from the encrypted data into one pixel of the cover; the given bit embeds in the Least Significant Bit of the blue byte of this pixel.

4-The Proposed Method

In this way the input message is divided into blocks each of which is 128 bit. The block is encrypted by using RC6 encryption algorithm. From the image (cover) a 16 bit will be taken and then rearranged into 4*4 array, the bits of the encrypted message are hidden in the diameter bytes of this array that means the encrypted bits will be hidden in LSB of iterated loop in brightness, red, green and blue of the hiding image. The encrypted bits will be extracted and then decrypted to check the hiding way. This modified method can be described as shown in Figure (4). The LSB method and the modified method will be used to hide the encrypted message, the comparison between the two methods are measured by using standard objective measures such as Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The results are shown in Tables (1) and (2).

5- System Evaluation Methods

Since the essential goal of steganography is the concealing of the fact that a secret message is transmitted, then it is very important to make the stego-file to be as close as possible to the cover-file. In fact, imperceptibility of the stego-file reflects how much it is affected due to the embedding process, in other words, imperceptibility can be decided by measuring that effect. In the proposed system, the MSE, PSNR and the Correlation Coefficient measurements are adopted.

5.1 Mean Squared Error (MSE)

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \| C(i,j) - S(i,j) \|^2$$

Where m and n are the number of rows and number of columns of the cover image respectively, C (i, j) is the pixel value from the cover image, S (i, j) is the pixel value from the stego-image [7].

5.2 Peak Signal to Noise Ratio (PSNR)

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

Here, MAX_I is the maximum pixel value of the image. When the pixels are represented using 8 bits per sample, this is **255**. More generally, when samples are represented using linear **PCM** with B bits per sample, MAX_I is 2^B-1.

5.3 The Correlation Coefficient Measuring Factor (The Similarity Test)

The similarity test is the correlation between the cover-image and stego-image. Correlation is one of the best known methods that evaluate the degree of closeness between two functions.

When the stego-image is perceptually similar to the original cover-image; then the correlation equals one.

Pearson Correlation Coefficient (Corr) is given by; [8]

$$Corr = \frac{\sum\sum(S-\overline{S})(C-\overline{C})}{\sqrt{\sum\sum(S-\overline{S})^2\sum\sum(C-\overline{C})^2}}$$

Where $\overline{S} = \frac{\sum\sum S}{MN}$.

S: stego-image. C: cover-image.

6. Results and Discussion

In this paper the tests are performed on text secret file using two types of hiding methods. The two hiding methods are Least Significant Bit and the modified method. In the LSB hiding method the embedding is in the least position, while the modified hiding method hides bits in LSB of iterated loop in brightness, red, green and blue of the hiding image.

Four different BMP images are used as cover files to embed the encrypted secret message using RC6 encryption method to obtain four different stego-files. These images are Cat.bmp, Lena.bmp, Lev.bmp, and Peppers.bmp.

Each one of figures (5, 6, 7 and 8) shows the original and histogram for the image, stego-files and histograms for stego-files when LSB embedding method and modified method are used.

As shown in histograms, cryptography techniques are used to increase the level of security and to make the system more complex to be defeated by attackers. The histograms of the four images are shown. The stego-file is to be as close to the cover-file as possible which means that the two methods are successful in hiding the message with more security.

The results of the three measuring factors for the two methods are given in Tables (1) and (2).

The output stego-file remains of the same size as the original file. It is also rarely affected after hiding the information according to objective measures or the objective measures (MSE and PSNR) as it appears in the results given in experimental result. These results prove that the goal of steganography is achieved where the stego-file will not look suspicious and nobody even knows that there is a hidden message.

The level of protection will be increased by using encryption algorithm. The proposed system for steganography is stronger against attack than any other existing system that does not use encryption. With the measuring of the (MSE) the minimum values are the better. The larger (PSNR) dB value is the higher image quality (which means there is only little difference between the cover-image and the stego-image), and with the measuring of the Correlation Coefficient the closer to one is the better. The results obtained from the correlation test indicate that the stego-file is similar in the two hiding methods since correlation values approach to one.

By studying of the whole system, it's clear that when the secret file size increases, MSE increases and the PSNR decrease. This result is obtained by applying different secret message sizes.

Hence a hacker must know the following in order to extract the embedded message from the stego-file:

a. Algorithm to extract the message from the image. (stego algorithm)

b. Encryption algorithm.

c. Correct password for algorithm.

7- Conclusion

In this paper four different BMP images are evaluated. These images are cat.bmp (Figure 5) as an example for an image containing large areas of a single color, Lena.bmp (Figure 6) as it is the reference image used in image processing research (it does not contain many high frequency components), Lev.bmp (Figure 7) and peppers.bmp (Figure 8) as examples of images containing many high frequency components.

With The (MSR), in Least Significant Bit we obtain maximum value (6.068E-2) and minimum value (6.068E-2) for all images. In the modified method we obtain maximum value (0.127), and minimum value (5.361E-03). The results for two hiding methods are very small.

With (PSNR), in Least Significant Bit the maximum value is (76.931), and minimum value is (60.317). In the modified method the maximum value is (70.856) and the minimum value is (57.109). In the two hiding methods we obtain large values of PSNR for all images which means there is only little difference between the cover-image and the stego-image.

the Correlation Coefficient measure gives values approaching to one which are better values. The Least Significant Bit gives a maximum of (0.99999987), and a minimum of (0.999991403), while the modified method gives a maximum of (0.99999947), and a minimum of (0.999983256), for all images. These results prove that the goal of steganography is achieved in the two hiding methods.

References:

[1] T. Morkel, J.H.P. Eloff and M.S. Olivier, "**An Overview of Image Steganography**", in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

[2] Maroney, C. Hide and Seek 5 for Windows 95, computer software and documentation, originally released in Finland and the UK, n.d. Downloadable from: http://www.rugeley.demon.co.uk/security/hdsk50.zip

[3] M. Owens, "**A Discussion of Covert Channels and Steganography**", as part of the Information Security Reading Room. SANS Institute 2002.

[4] A. H. Ouda and M. R. El-Sakka, "**A Step Towards Practical Steganography Systems**", Computer Science Department, University of Western Ontario, London, Ontario, Canada, ICIAR 2005, LNCS 3656, pp. 1158 – 1166, 2005.

[5] A. Setiawan, D. Adiutama, J. Liman, A. Luther and R. Buyya," **Grid Crypt: High Performance Symmetric Key Cryptography using Enterprise Grids**", Grid Computing and Distributed Systems Laboratory**,** Dept. of Computer Science and Software Engineering**,** The University of Melbourne, Australia,2004.

[6] N. Sharma, J. S. Bhatia, N. Gupta, "**An Encrypto-Stego Technique Based Secure Data Transmission System**",The Infosec Writers Text Library (RSS) , 2005.

[7] Ashwaq T. Hashim **"Type-3 Feistel Network of The 128-bits Block Size Improved Blowfish Cryptographic Encryption**", Eng & Tech, Journal, Vol. 27, No. 2, 2009.

[8] Venkatraman. S, A. Abraham and M. Paprzycki, "**Significance of Steganography on Data Security**", Dept. of Computer Science & Engineering, University of Madras, INDIA, Dept. of Computer Science, Oklahoma State University, USA, Proceedings of the International Conference on Information Technology, 2004IEEE.

Table (1) System evaluation when using LSB embedding method

Image	MSE	PSNR	CORRELATION
Cat	9.405E-03	68.414	0.999998967271495
Lena	6.068E-2	60.317	0.999991403088456
Lev	1.323E-03	76.931	0.999999870254599
Peppers	5.298E-03	70.906	0.999999284715728

Table (2) System evaluation when using the modified method

Image	MSE	PSNR	CORRELATION
Cat	3.184E-02	63.118	0.99999654160075
Lena	0.127	57.109	0.999983256264233
Lev	5.361E-03	70.856	0.999999479693163
Peppers	2.151E-02	64.821	0.999997131589161

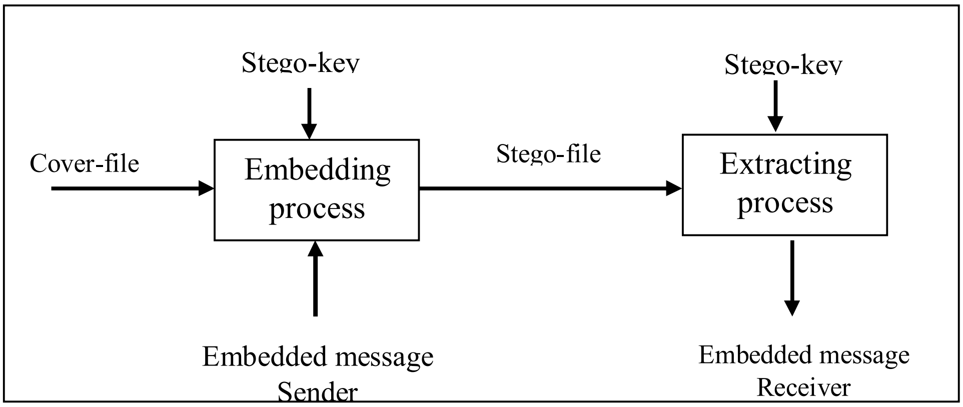


Figure (1) Framework of the embedding process

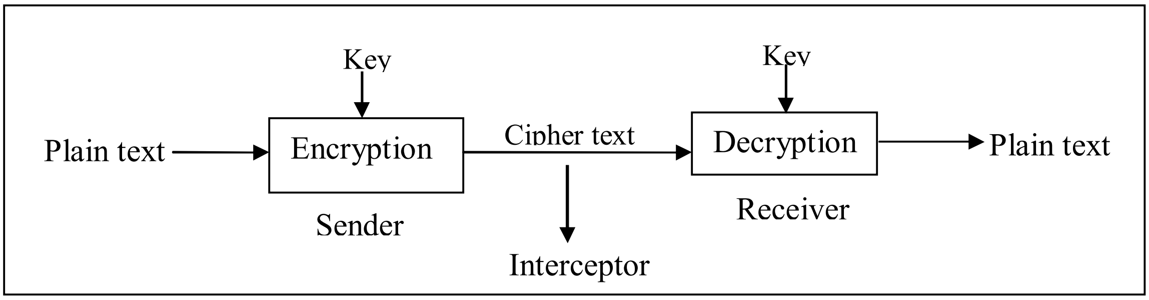


Figure (2) Block diagram of ciphering system

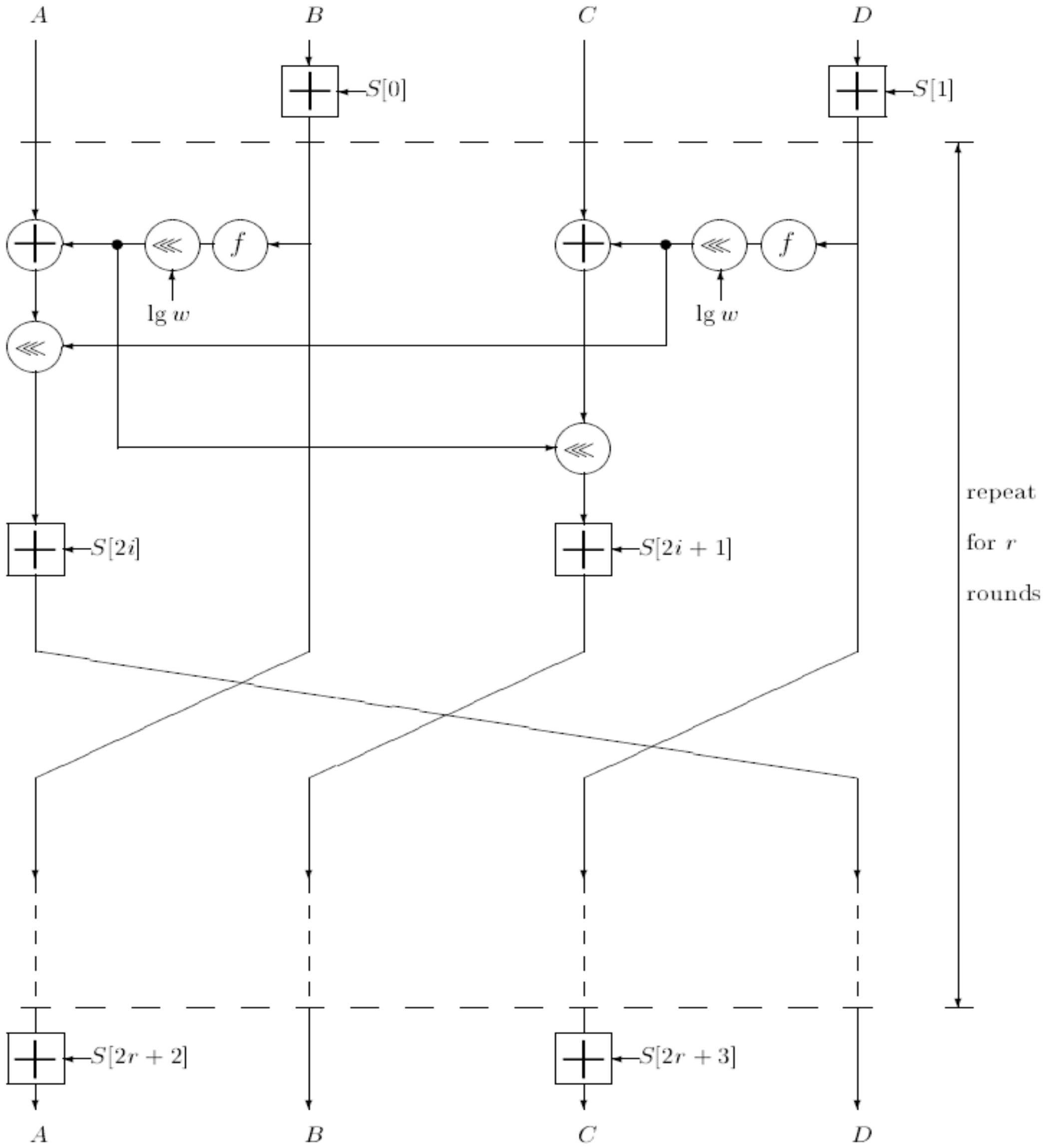


Figure (3) Encryption with RC6-w/r/b. Here f(x) =x (2x+1)

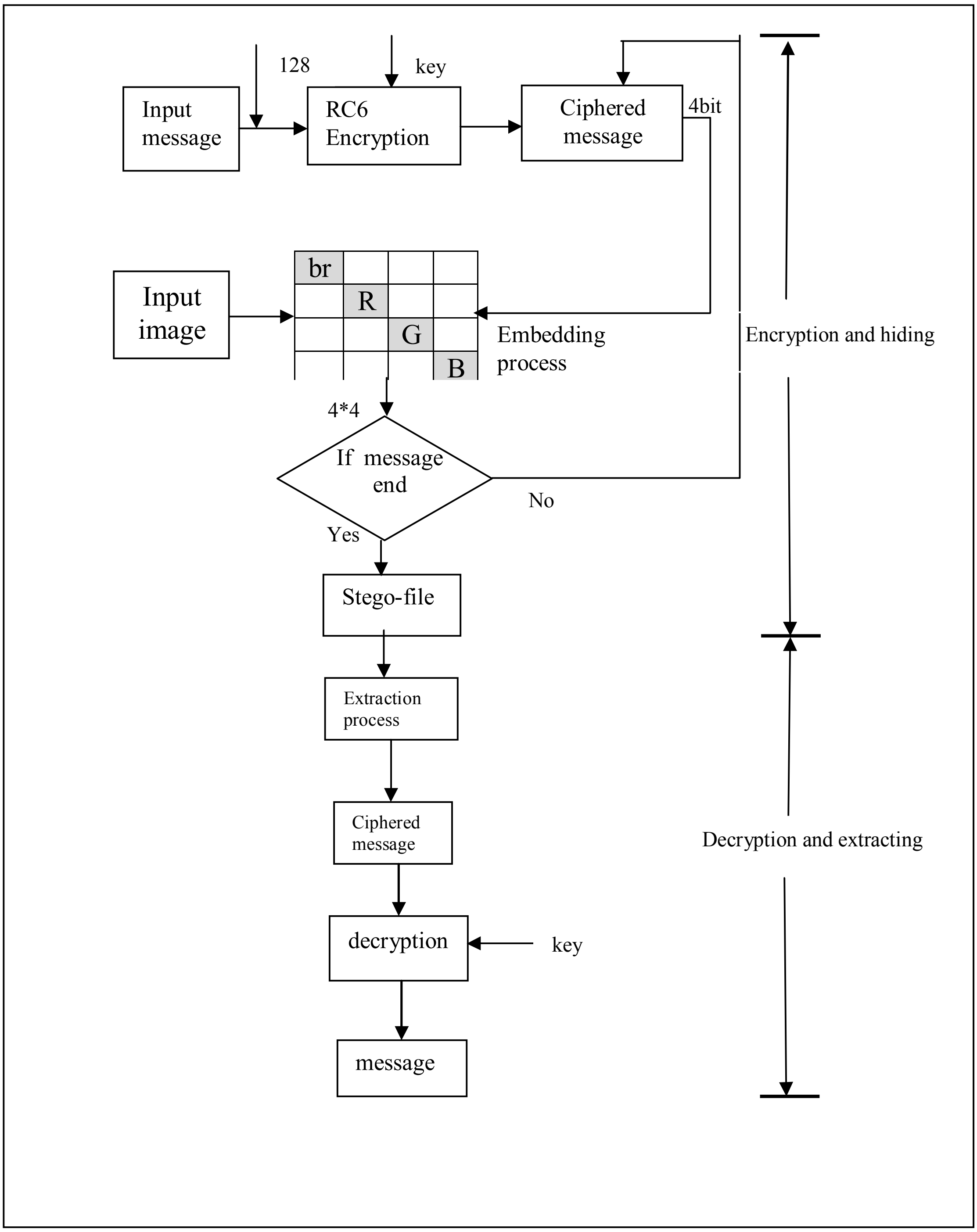


Figure (4) The flowchart of the modified method.

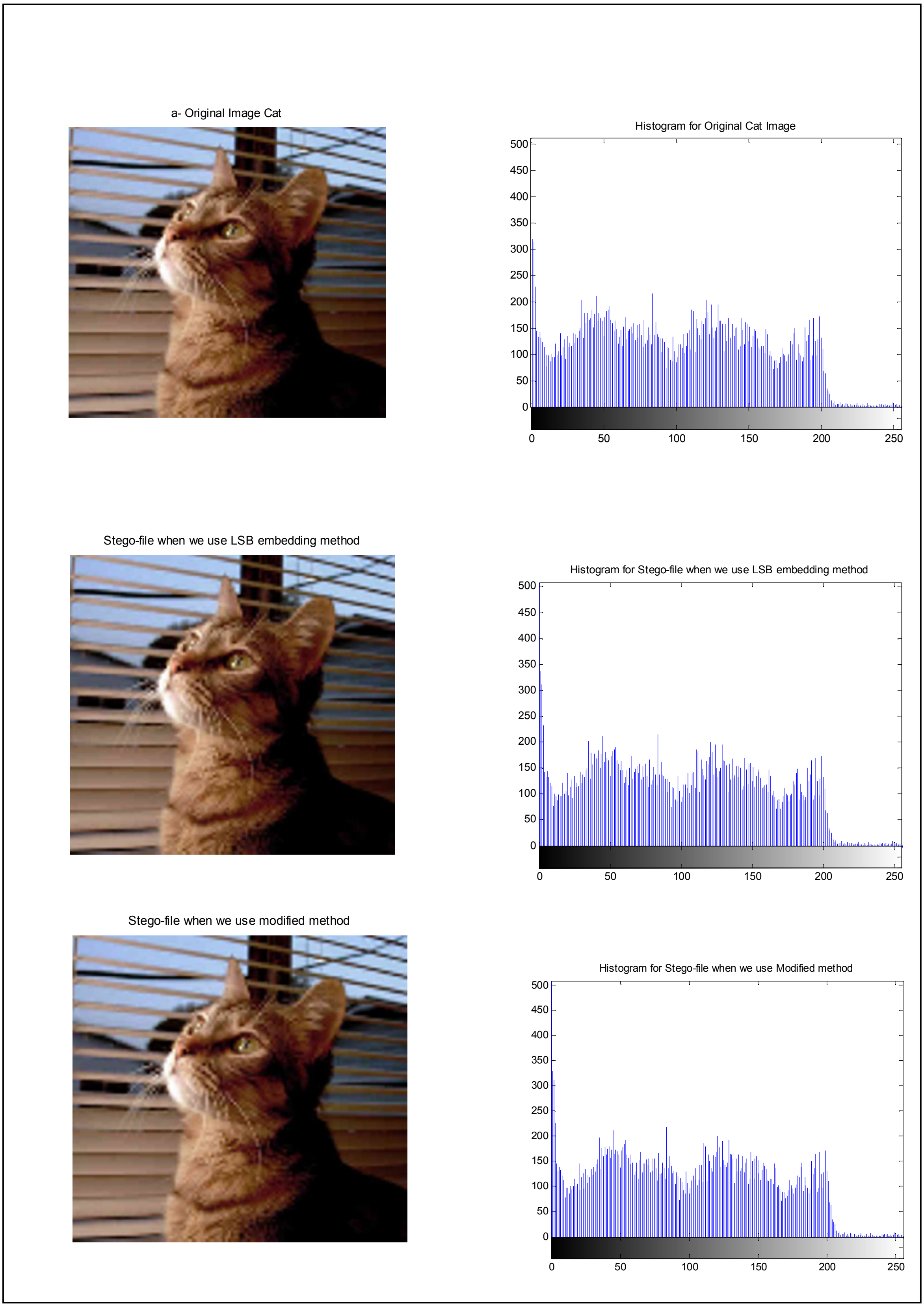


Figure (5) The original and histogram for Cat image, stego-files and histograms when LSB embedding method and modified method are used.

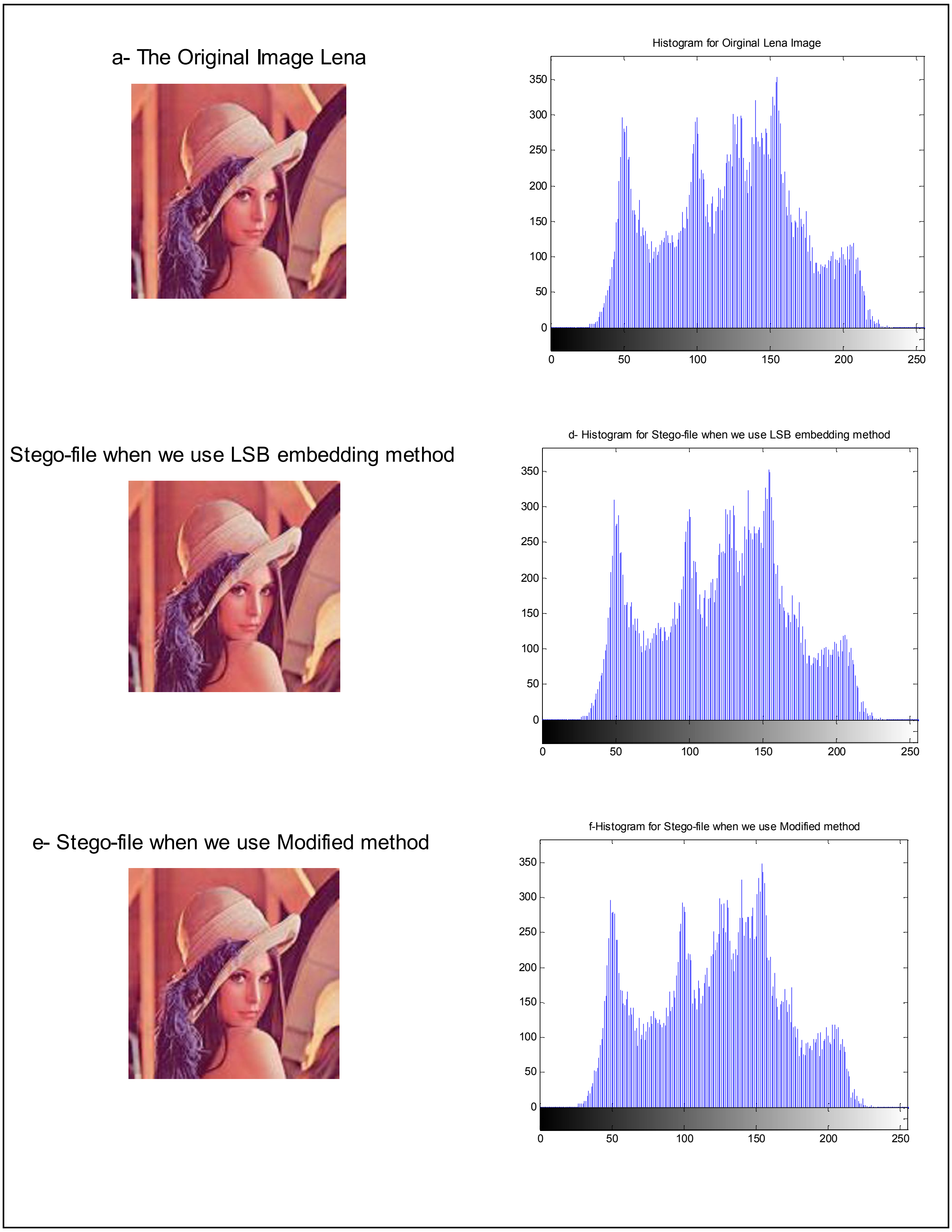


Figure (6) The original and histogram for Lena image, stego-files and histograms when LSB embedding method and modified method are used.

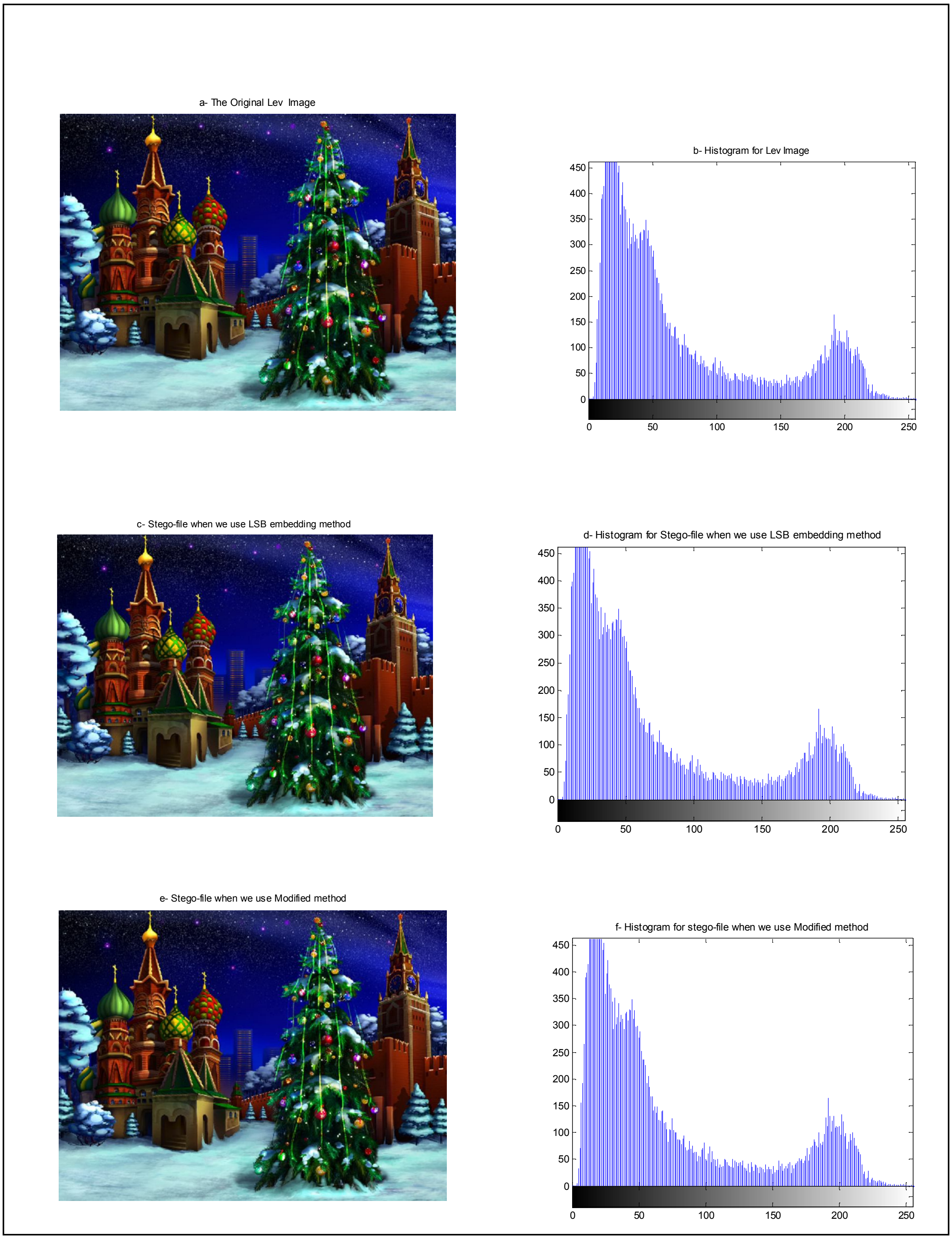
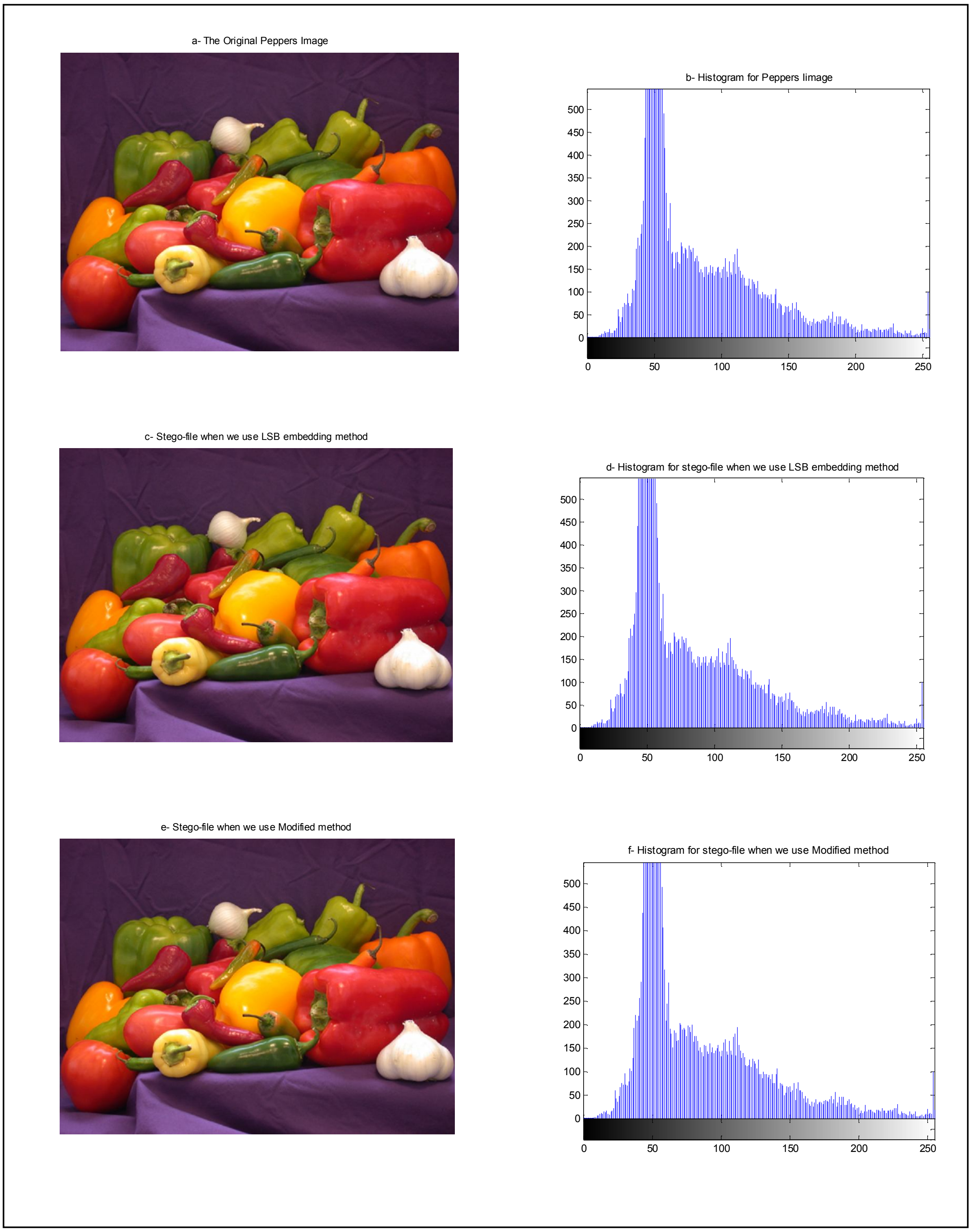


Figure (7) The original and histogram for Lev image, stego-files and histograms when LSB embedding method and modified method are used.



a- The Original Peppers Image

b- Histogram for Peppers Iimage

c- Stego-file when we use LSB embedding method

d- Histogram for stego-file when we use LSB embedding method

e- Stego-file when we use Modified method

f- Histogram for stego-file when we use Modified method

Figure (8) The original and histogram for Peppers image, stego-files and histograms when LSB embedding method and modified method are used.