Eng. & Tech. Journal, Vol. 27 ,No. 13 , 2009

Enhancing Embedded Data Security By Turns Cipher Block Chaining Mode Into Stream Cipher

Salah Mahdi Saleh*

Received on:1/7/2008
Accepted on:7/5/2009

Abstract

In this paper, a secure data hiding method is introduced. It increases the security of embedded data through combining between the steganography and cryptography. First, the secrete message is divided into blocks with same size according to length of key stream that is generated using nonlinear key generator. This key is used to encrypt the first block in secret message using the stream cipher, whereas the other blocks are encrypted depending on the behavior of cipher block chaining (CBC) mode that turn on the stream cipher in order to guarantee no duplicated encrypted blocks. In our CBC mode the current ciphertext block will became a key stream to encrypt the next plaintext block, and so on. After encryption stage complete, the encrypted massage are embedded randomly in bmp image using LSB insertion method to increase the security.

Keywords: Steganography; cryptography; CBC mode; stream cipher; LSB insertion

تحسين أمنية البيانات المخفية بتحويل صيغة سلسلة قطاع التشفير إلى التشفير الانسيابي

الخلاصة

قدّمت في هذا البحث طريقة إخفاء بيانات آمنة. إنها تزيد من أمنية البيانات المخفية من خلال الجمع بين الإخفاء والتشفير. تقسّم الرسالة أولاً إلى قطاعات متساوية الحجم طبقاً لطول سلسلة مفتاح يتم توليدها باستعمال مولد مفاتيح خطي. يستعمل هذا المفتاح لتشفير القطاع الأول في الرسالة السرية باستخدام التشفير الانسيابي، بينما تُشفر القطاعات الأخرى اعتماداً على سلوك صيغة سلسلة قطاع التشفير التي تحوّل إلى التشفير الانسيابي لكي تضمن عدم ظهور قطاعات مشفرة مكررة. ففي طريقة سلسلة قطاع التشفير المستعملة في بحثنا يصبح قطاع التشفير الحالي كسلسلة مفتاح لتشفير قطاع النص الصريح التالي. بعد ذلك يتم إخفاء الرسالة المشفرة عشوائياً في صورة bmp باستعمال طريقة حشر الثنائيات الأقل أهمية لزيادة الأمنية.

*College of Sciences for Women, Babylon university/ Babylon

https://doi.org/10.30684/etj.27.13.14
2412-0758/University of Technology-Iraq, Baghdad, Iraq
This is an open access article under the CC BY 4.0 license http://creativecommons.org/licenses/by/4.0

1. Introduction

Steganography is a means of storing information in a way that hides information's existence. Steganography contains the techniques for secret hiding of messages in another wise innocent looking carrier message. The purpose of steganography is not to keep others from knowing the hidden information, but is to keep others from thinking that the information even exists [1]. Therefore, the main goal is to not raise suspicion and avoid introducing statistically detectable modifications into the carrier media [2][3][4].

Historically, the first steganography techniques included invisible writing using special inks or chemical[5]. Today, it seems natural to use digital images, digital video, or audio for hiding secret message[6]. Currently, there are two directions within steganography [7]: one of them is used for protection against detection, while another is used for protection against removal (i.e. stegaography and watermarking, respectively).

One of the most common uses of modern steganography in digital world of computers is to hide information from one file in the contents of another file[8] .

In the field of steganography, some terminology has been developed, as explained below. The term **"cover"** is used to describe the original, innocent message, data, audio, still, video and so on. The information to be hidden in the cover data is known as the **"embedded"** data. The **"stego"** data is the data containing both the cover signal and the "embedded" information. Logically, the processing of putting the hidden or embedded data, into the cover data, is sometimes known as embedding. Occasionally, especially when referring to image steganography, the cover image is known as the *carrier*.

The aim of cryptography is not to hide the existence of a message, but rather to hide or conceal its meaning [9][10]. With cryptography you start off with a plaintext message, which is a message in its original form. You then use an encryption algorithm to garble a message, which creates ciphertext. You would then use a decryption algorithm to take the cipher image steganography, the cover image is known as the *carrier*.

The aim of cryptography is not to hide the existence of a message, but rather to hide or conceal its meaning [9][10]. With cryptography you start off with a plaintext message, which is a message in its original form. You then use an encryption algorithm to garble a message, which creates ciphertext. You would then use a decryption algorithm to take the ciphertext and convert it back to a plaintext message. During the encryption and decryption process, what protects the ciphertext and stops someone from inadvertently decrypting it back to the plaintext message is the key [9]. Therefore the secrecy of the ciphertext is based on the secrecy of the key, not the

PDF created with pdfFactory Pro trial version www.pdffactory.com

secrecy of the algorithm.Ciphers can either encrypt data a single character at a time (stream ciphers) or a number of characters at a time (block ciphers) [11]. As opposed to a block cipher, a stream cipher encrypts the message a bit of text at a time. This means that a stream cipher breaks a message down into 1’s and 0’s before the message is encrypted. To encrypt the stream of 1’s and 0’s from the message, the stream cipher uses a component known as a key stream generator. The key is then input into the key stream generator to generate a stream of random 1’s and 0’s. The original message is then put through a mathematical process known as exclusive ORing (X-OR) where the two bits are compared. If the bit from the original message is a 1 and the bit from the key stream generator is a 1, then the encrypted message would send out a 0 or the first bit. If the two bits are the same, the X-OR process yields 0; if the two bits are different, the process yields a 1Because the randomness of the 1’s and 0’s coming from the key stream generator is critical to the security of a stream cipher, there are rules that must apply to a key stream generator [11]. A key stream generator must have long periods where the key stream does not repeat. The key stream must be functionally complex, which means that the key stream cannot be the key and then the key in reverse and then the key. The key stream must be statistically unpredictable, which means there are no patterns to the key stream. The key stream must be unbiased, which means there are as many 1’s as 0’s. The key stream cannot be easily related to the key. All of these rules increase the security and secrecy of a stream cipher. original message is then put through a mathematical process known as exclusive ORing (X-OR) where the two bits are compared. If the bit from the original message is a 1 and the bit from the key stream generator is a 1, then the encrypted message would send out a 0 or the first bit. If the two bits are the same, the X-OR process yields 0; if the two bits are different, the process yields a 1.

Because the randomness of the 1’s and 0’s coming from the key stream generator is critical to the security of a stream cipher, there are rules that must apply to a key stream generator [11]. A key stream generator must have long periods where the key stream does not repeat. The key stream must be functionally complex, which means that the key stream cannot be the key and then the key in reverse and then the key. The key stream must be statistically unpredictable, which means there are no patterns to the key stream. The key stream must be unbiased, which means there are as many 1’s as 0’s. The key stream cannot be easily related to the key. All of these rules increase the security and secrecy of a stream cipher.

Furthermore, there is a requirement that the key stream must not be repeated [12] (stream cipher must be one-time pad). A one-time pad is a method of encoding a message with a random key is an unbreakable system because no matter how much time or sample text a cryptanalyst has available, breaking the code would be impossible [13]. The cipher would never be the same twice. Similarly

PDF created with pdfFactory Pro trial version www.pdffactory.com

we should use a stream cipher key only once.

With a block cipher, we can reuse keys. When it becomes necessary to encrypt many things using the same key, block cipher proves to be stronger. The different modes of operation turns a block cipher into a stream cipher [10]. They can be proven secure under the assumption that the block cipher is secure.

The rest of this paper is organized as follows. Section 2 reviews the comparison between steganography and cryptography. Section 3 contains the linear feedback shift register. The new scheme is presented in Section 4. Implementation results are in Section 5. Conclusions are drawn in Section 6.

2.Cryptography and steganography: A comparison

Cryptography and steganography are different. While cryptography techniques attempting to conceal the content of messages, steganography is about concealing their very existence [142]

once and only once. This type of encoding is an unbreakable system because no matter how much time or sample text a cryptanalyst has available, breaking the code would be impossible [13]. The cipher would never be the same twice. Similarly we should use a stream cipher key only once.

With a block cipher, we can reuse keys. When it becomes necessary to encrypt many things using the same key, block cipher proves to be stronger. The different modes of operation turns a block cipher into a stream cipher [10]. They can be proven secure under the assumption that the block cipher is secure.

The rest of this paper is organized as follows. Section 2 reviews the comparison between steganography and cryptography. Section 3 contains the linear feedback shift register. The new scheme is presented in Section 4. Implementation results are in Section 5. Conclusions are drawn in Section

2. Cryptography and steganography: A comparison

Cryptography and steganography are different. While cryptography techniques attempting to conceal the content of messages, steganography is about concealing their very existence [14] [15]. Steganography hides a message within another message and looks like a normal graphic, video, or sound file. In Cryptography, the message is encrypted; looks like a meaningless jumble of characters [13]. Cryptography techniques used to scramble a message so that if it is discovered it cannot be read. A cryptography messages are difficult or impossible to understand and decode. Steganography hides the existence of a message so that if successful it generally attracts no suspicion at all. A message in cipher text may arouse suspicion while an invisible message will not.

Whenever you consider two or more technologies to be used in your communication security strategy, you should determined whether they

PDF created with pdfFactory Pro trial version www.pdffactory.com

are complementary or competing. If they are competing , that means they both do the same thing and the technologies are redundant. If they are complementary, they provide different services (by putting them together you obtain a more robust result) [16]. Some steganographic methods combine traditional cryptography with steganography [9][17]. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plaintext is in the carrier medium. Therefore, In order to increase the security of the over all communication process and maximize the efficiency of both techniques encryption is recommended in conjunction with steganography [6].

3. Linear feedback shift register [10]

A linear feedback shift register (LFSR) of length n over the finite field F_q consists of n stages $[s_{n-1}, s_{n-2}, . . . , s_0]$ with si ∈ F_q, The register is controlled by a clock, and at each stepping the elements are moved to normal graphic, video, or sound file. Cryptography, the message is encrypted; looks like a meaningless jumble of characters [13]. Cryptography techniques used to scramble a message so that if it is discovered it cannot be read. A cryptography messages are difficult or impossible to understand and decode. Steganography hides the existence of a message so that if successful it generally attracts no suspicion at all. A message in cipher text may arouse suspicion while an invisible message will not.

Whenever you consider two or more technologies to be used in your communication security strategy, you should determined whether they are complementary or competing. If they are competing , that means they both do the same thing and the technologies are redundant. If they are complementary, they provide different services (by putting them together you obtain a more robust result) [16]. Some steganographic methods combine traditional cryptography with steganography [9][17]. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plaintext is in the carrier medium. Therefore, In order to increase the security of the over all communication process and maximize the efficiency of both techniques encryption is recommended in conjunction with steganography [6] noted that all proposals based only on these methodologies have been broken.

3.1 Nonlinear combination generators

A nonlinear combination generator uses several maximum-length LFSRs (see Figure 1.a). The key stream is generated as a nonlinear Boolean function *f* of the outputs of these LFSRs. The function *f* is called the combining function.

3.2 Nonlinear filter generators

A nonlinear filter generator uses a single maximum-length LFSR, and the key keystream is generated as a nonlinear

PDF created with pdfFactory Pro trial version www.pdffactory.com

3.3 Clock-controlled generator

A Clock-controlled generator consists of at least one LFSR, which is irregularly clocked by some other part of the cipher. In the alternating step generator, the output of one LFSR decide which one of the other two LFSRs that should be clocked. In the shrinking generator, two LFSRs are regularly clocked. If the output of the first LFSR is 1, the output of the second forms part of the keystream.

4-The Proposed enhancing algorithm

Ensuring data security is a big challenge for computer users. Businessmen, professionals, and home users all have some important data that they want to secure from others. There are a number of ways for securing data. Encryption and steganography are employ to them. Those two methods have been used together in the proposed algorithm to increase the security of the data. First we will encrypt the secrete message by using the stream cipher and then embed the result (ciphertext) in an image file. This algorithm will improves the security of the data by embedding an encrypted text rather than plaintext in an image.

4-1 Encryption

The encryption procedure that used is a cipher block chaining (CBC) mode turns to stream cipher. When we give this procedure a chunk of data, it breaks the plaintext (after converting it to a sequence of bits) into blocks according to the length of key stream that used which supplied by the key generator (nonlinear filter generators). After that, the encryption procedure runs with CBC mode. In this mode we will generate the current ciphertext block from XORing the vector is XOR ed with the current has to apply the same algorithm that used to embed the message in order to retrieve it. However, if he finds out that algorithm, he could get back only the ciphered massage. In this ciphered massage he could see nothing but the junk characters. This provides an extra layer of protection. To get the original massage, those junk character must be decrypted with the encryption algorithm and the correct key stream. This also add an extra layer of protection. Furthermore, to get the correct key stream he must know the structure of key generator (including linear feedback function, initial state, and the nonlinear function to get the bits stream). This add another layer (s) of protection making the attacker have to face difficulties in him mission to get the secrete message. Furthermore, LSB hiding algorithm selects each position (pixel) according to a random number. This process of generating random numbers depends on a value (seed). Therefore the hacker, if he knows the hiding algorithm, must finds that seed in order to get the correct hiding positions. This will add an extra layer of protection.

4-2 Hiding

This part of proposed algorithm hides encrypted text into a carrier medium using the least significant bit (LSB) insertion technique (for more details about LSB method you can refer to [13]). After that, the stego medium will be

PDF created with pdfFactory Pro trial version www.pdffactory.com

resulting, which represents by a BMP file. The message is hidden into two LSBs of each pixel of the image file. Since a very small changes in the stego-image, this algorithm does not reveal the fact that it contains some data (makes the change is unnoticeable).

LSB selects each pixel to hide a two bits from a message according to a random number. The step of getting a random number is depending on a seed. This will adding another layer of security.

4-3 Levels of security in the proposed algorithm

The attacker (hacker) can see the stego image along with the message embedded into it. If the stego image does not reveal any difference in attributes (like size, content, and etc.) from that of the original image, it is difficult for an attacker to find out that this image contains a message.

Even if he notices or doubts that, he has vector is XOR ed with the current plaintext block to generate the ciphertext block.

4. For other iterations:

i. Initialization vector is set to the current ciphertext block.

ii. The current plaintext block is XOR ed with the previous ciphertext block to generate the current ciphertext block.

..

5-The results

To stand on performance of the proposed method, we are applied it to hide an audio messages (WAV format) in 8 bit/pixel gray and color images (BMP format) with size (128×128) by using LSB insertion method. We are used subject and object criteria in the comparing process. In object criteria, the peak signal to noise ratio (**PSNR**) formula is used as follow:

$$PSNR = 10\log_{10}\frac{(L-1)^2}{\frac{1}{M\times N}\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[\hat{I}(r,c)-I(r,c)\right]^2} \quad \mathbf{K}(4)$$

where L represent the number of gray levels, $\hat{I}$ is the stego-image, and I is cover-image with size (MxN).

Each experiment before hiding determines three components, these are: the structure of key generator, the randomize seed, and the length of key stream that used. We will refer to each stage in shift register by x_i, where i=1…n and n is the length of shift register.

PDF created with pdfFactory Pro trial version www.pdffactory.com

5-1 Hiding an audio message in gray images.

In this experiment we will embedding an audio message with size (3.89 KB) in gray images. The length of shift register is 16 stages. The linear function for feedback is obtained as follow:

$$f(x) = x_1 \oplus x_6 \oplus x_9 \oplus x_{13} \oplus x_{16}$$

The nonlinear filtering function to obtain the key stream is as follow:

$f(x) = x_1x_6x_{15} + x_2x_4x_{11} + x_3x_7x_{13} + x_5x_8x_{10}$

The length of key stream is (1500) and the seed for generating random positions is (6). The results of **PSNR** is explained in the table (1).

The cover-images and stego-images for tables 1 appear in appendix (A). Observe the table 1 shown above. The values of **PSNR** performed is ranged in the interval of 44.243 ~ 44.353. It's acceptable to human vision's imperceptibility. This makes the embedded message undistinguished.

5-2 Hiding an audio message in 8 bits/pixel colors images

In this experiment we will embedding an audio message with size (3.89 KB) in 8 bits/pixel colors images. The length of shift register is 16 stages. The linear function for feedback is obtained as follow:

$$f(x) = x_2 \oplus x_5 \oplus x_9 \oplus x_{12} \oplus x_{16}$$

The nonlinear filtering function to obtain the key stream is as follow:

$f(x) = x_1x_6x_{15} + x_4x_{11} + x_3x_7x_{13} + x_5x_8x_{10}$

The length of key stream is (1300) and the seed for generating random positions is (6). The results of **PSNR** is explained in the table (2).

The cover-images and stego-images for tables 2 appear in appendix (B). You can see from the results of **PSNR** which appear in table (2) that the changes in images can not recognize. This makes the stego-image undistinguished.

In this experiment we will explaining the results of hiding when using different values for seed. It embeds an audio message with size (1.79 KB) in gray images. The length of shift register is 10 stages. The linear function for feed back is obtained as follow:

$$f(x) = x_3 \oplus x_5 \oplus x_{10}$$

The nonlinear filtering function to obtain the key stream is as follow:

$f(x) = x_2x_4 + x_1x_6 + x_3x_7 + x_5x_8$

The length of key stream is (1000) and the seeds for generating random positions is 5 and 7 respectively. The results is explained in the table (3).

The cover-images and stego-images for tables 3 appear in appendix (C). As you see from table 3, the values of **PSNR** is differed when we using different values for randomize seed. Therefore, this seed adds level of security to the embedded algorithm because, in order to extract the embedded

PDF created with pdfFactory Pro trial version www.pdffactory.com

message, we must reach the correct position and without that seed can not do that. The hacker will face a problem in determining that positions.

6-Conclutions

In this paper, a novel and efficient steganographic method is proposed to embed encrypted information within an image data randomly. This method will be expected to spread hidden information within image data randomly before transmission. The CBC mode will be guarantee that any duplicated block in the plaintext does not encrypted to the same ciphertext block. In this way the security level of stream cipher has been increased. The insertion positions of secret information will be randomly selected depending on a seed and the results will be vary if the seed change, which adds a layer of protection. Since a very small changes in the stego-image as a result to use the LSB algorithm, it does not reveal the fact that it contains some data and makes the changes are unnoticeable. Experimental results also show that the PSNR values prove that the quality of seed change, which adds a layer of protection. Since a very small changes in the stego-image as a result to use the LSB algorithm, it does not reveal the fact that it contains some data and makes the changes are unnoticeable. Experimental results also show that the PSNR values prove that the quality of stego-image is acceptable to human vision system and makes the embedded message is undistinguished.

References

[1] D. Artz. Digital Steganography :Hiding Data within Data. IEEE INTERNET COMPUTING, Vol. 5, No. 3, pp. 75-80, MAY/JUNE, 2001.

[2] S. Lyu and H. Farid. Steganalysis Using Higher-Order Image Statistics. IEEE Transactions on Information Forensics and Security, Vol. 1, No. 1, pp. 111-119, March, 2006.

[3] J. Fridrich and D. Rui. Secure Steganography Methods for Palette Images. Proceedings of the third International Workshop on Information Hiding, Lecture Notes In Computer Science, Vol. 1768, pp. 47-60, London, UK, 1999.

[4] S. Katzenbeisser and F. A. P. Petitcolas. Defining Security in Steganographic Systems. Proceedings of Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, Vol. 4675, pp. 50-56, San Jose, CA, USA, 21-24 January, 2002.

[5] D. Kahn. The history of steganography. Proceedings of the first Workshop on Information Hiding, Lecture Notes In Computer Science, Vol. 1174, pp. 1-5, 30 May –1 June, Cambridge, UK, 1996.

[6] J. Fridrich. A New Steganographic Method for Palette–Based Images. Proceedings of the IS&T's PICS conference, pp. 285-289, April, Savannah, Georgia (1999).

PDF created with pdfFactory Pro trial version www.pdffactory.com

[7] L. M. Marvel and C. T. Retter. The Use of Side Information in Image Steganography. Proceedings of the IEEE International Symposium on Information Theory and Its Applications (ISITA'2000), Honolulu, HI, November, 2000.

[8] K. Rabah. Steganography –The Art of Hiding Data. Information Technology Journal 3(3), pp. 245-269 , 2004 .

[9] E. Cole and S. Ring. Insider Threat Protecting the Enterprise from Sabotage, Spying, and Theft. Syngress Publishing, Inc. Canada. 2005.

[10] J. Mattsson. Stream Cipher Design: An evaluation of the eSTREAM candidate Polar Bear. Master of Science Thesis. Royal Institute of Technology. Sweden. 2006.

[11] T. R. Peltier, J. Peltier and J. Blackley. Information Security Fundamentals. CRC Press LLC. USA. 2005.

[12] A. Uhl and A. Pommer. Image and Video Encryption: From Digital

Rights Management to Secured Personal Communication. Springer. USA. 2005.

[13] G. Kipper. Investigator's Guide to Steganography. CRC Press LLC. USA. 2004.

[14] R.J. Anderson and F. A. P. Patitcolas. On The Limits of Steganography. IEEE jornal of selected. 1998.

[15] K. Curran and K. Bailey. An Evaluation of Image Based Steganography Methods.2003.

[16] E. Cole. Hiding In Plain Sight: Steganography and the Art of Covert Communication. Wiley Publishing Inc..USA. 2003.

[17] S. Katzenbeisser and F. A. P. Petitcolas. Information hiding techniques for steganography and digital watermarking. ARTECH HOUSE, INC. USA. 2000.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Table 1: The results of PSNR for the stego-images.

Cover image	PSNR
Lenna	44.3 db
Mand	44.243 db
Peppers	44.353 db
Goldhill	44.316 db

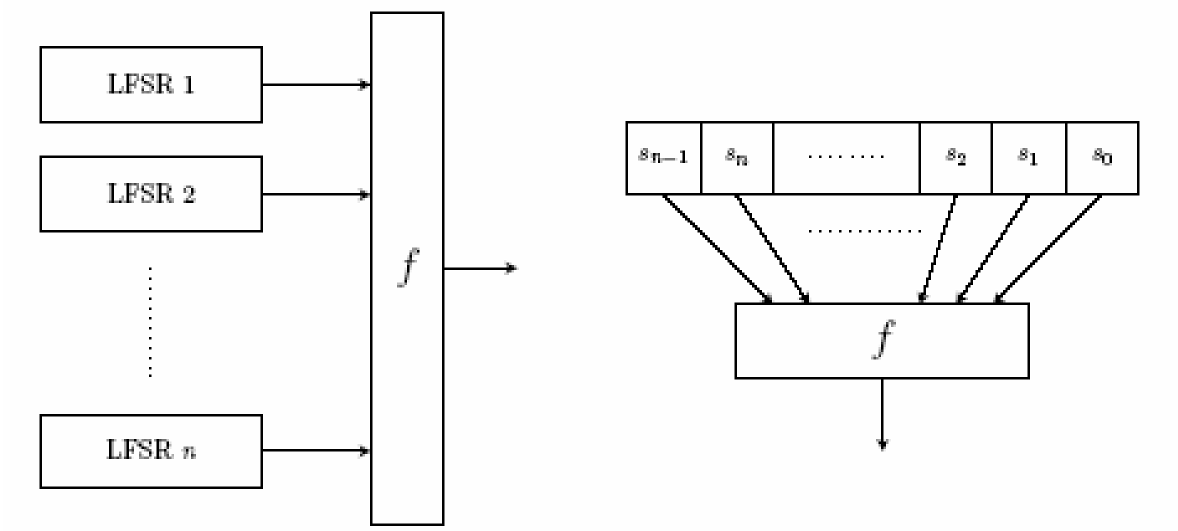
Table 2: The results of PSNR for the stego-images.

Cover image	PSNR
Tree	44.482 db
Cat	44.334 db
Garden	44.242 db
Fly	44.224 db

Table 3: The results of PSNR for the stego-images.

Cover image	Seed=5	Seed=7
Lenna	47.526 db	47.501 db
Mand	47.606 db	47.561 db
Peppers	47.691 db	47.713 db
Goldhill	47.536 db	47.524 db

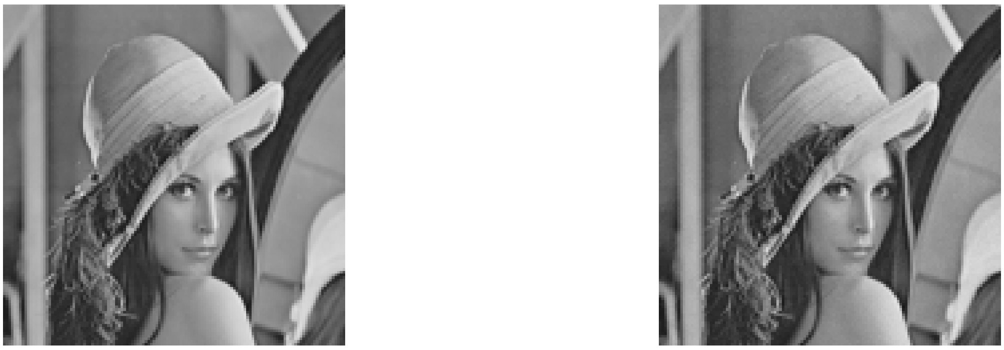
PDF created with pdfFactory Pro trial version www.pdffactory.com



(a) (b)

Figure 1: (a) Nonlinear combination generator, and (b) nonlinear filter generator

Appendix A



(a (b

Figure 2. lenna image, (a) cover-image and (b) stego-image.

PDF created with pdfFactory Pro trial version www.pdffactory.com

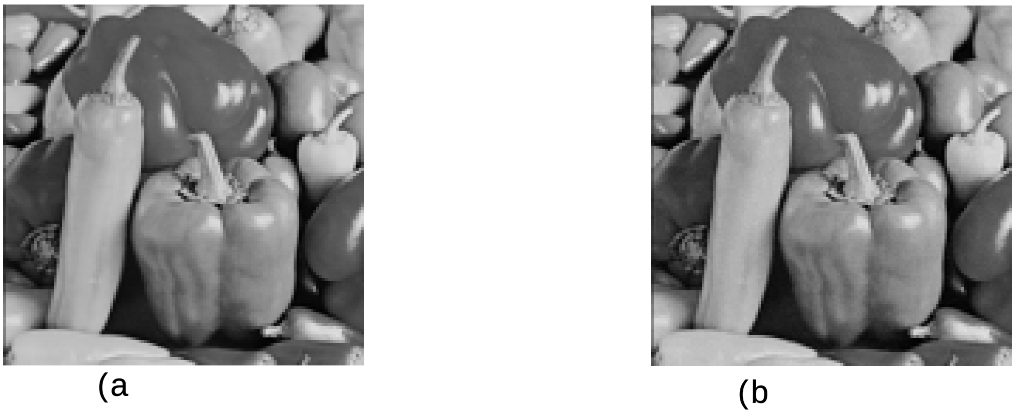


Figure 3. mand image, (a) cover-image and (b) stego-image.

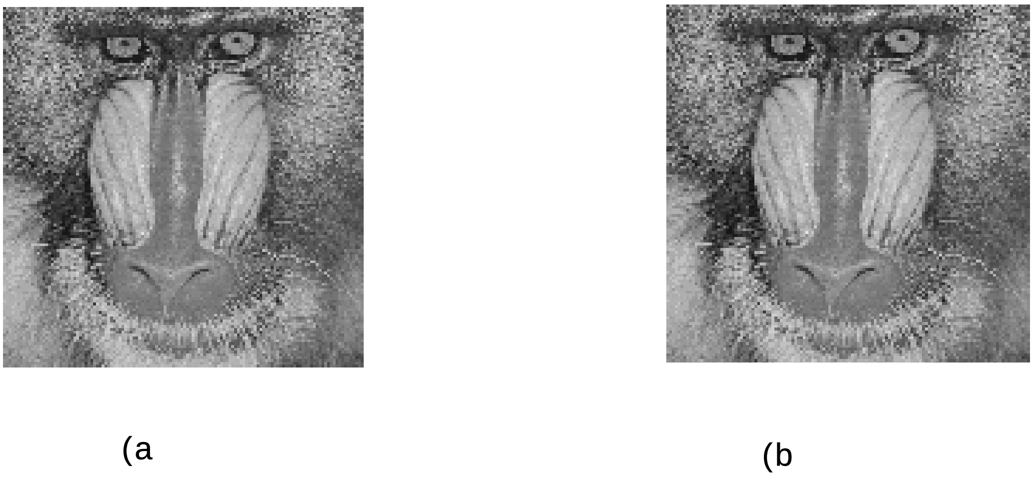


Figure 4. peppers image, (a) cover-image and (b) stego-image.

PDF created with pdfFactory Pro trial version www.pdffactory.com

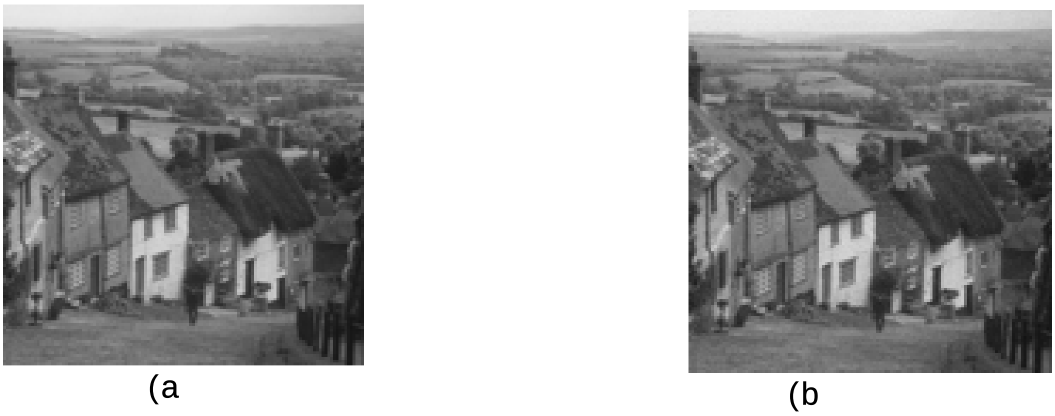


Figure 5. goldhill image, (a) cover-image and (b) stego-image.

Appendix B

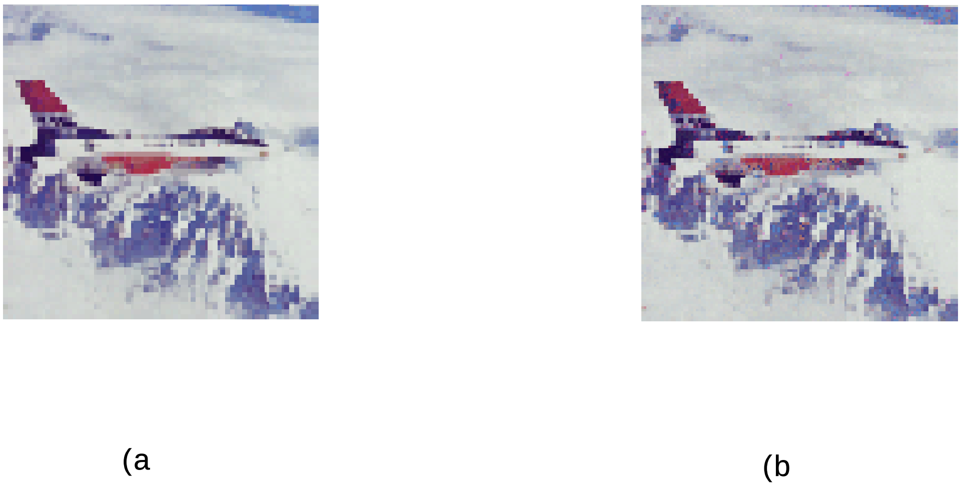


Figure 6. fly image, (a) cover-image and (b) stego-image.

PDF created with pdfFactory Pro trial version www.pdffactory.com

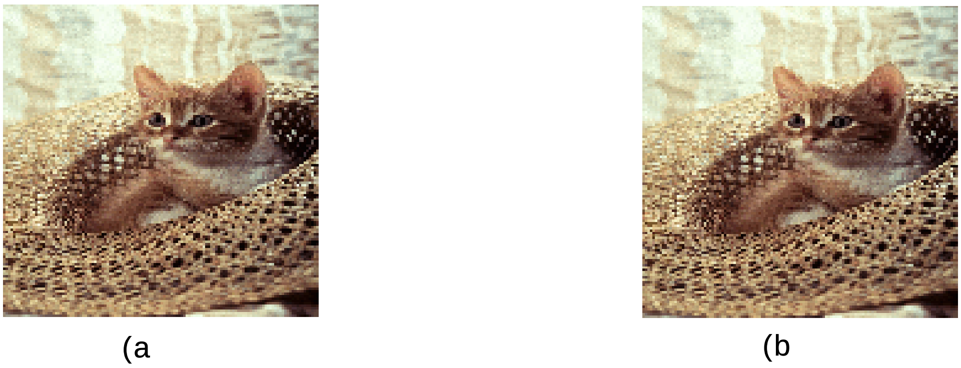


Figure 7. cat image, (a) cover-image and (b) stego-image.

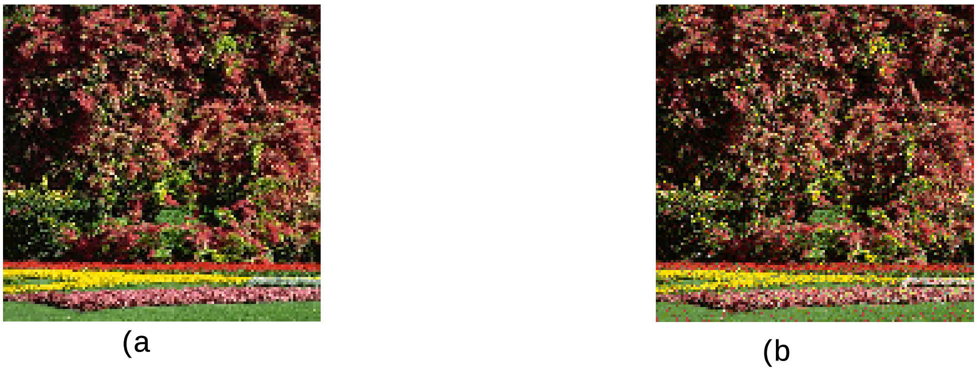


Figure 8. garden image, (a) cover-image and (b) stego-image.

Figure 9. tree image, (a) cover-image and (b) stego-image.

PDF created with pdfFactory Pro trial version www.pdffactory.com

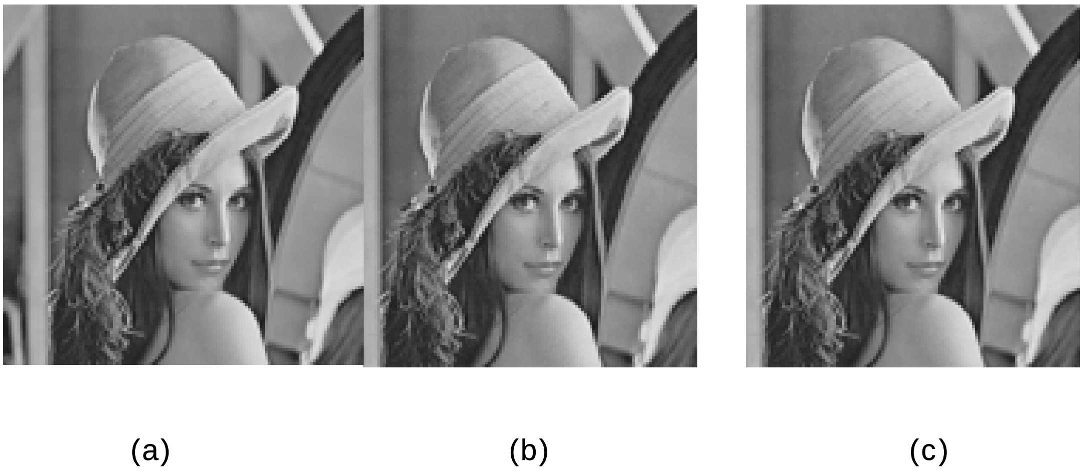


Figure 10. lenna image. (a) cover-image, (b) stego-image with seed=5, and (c) stego-image with seed=7.

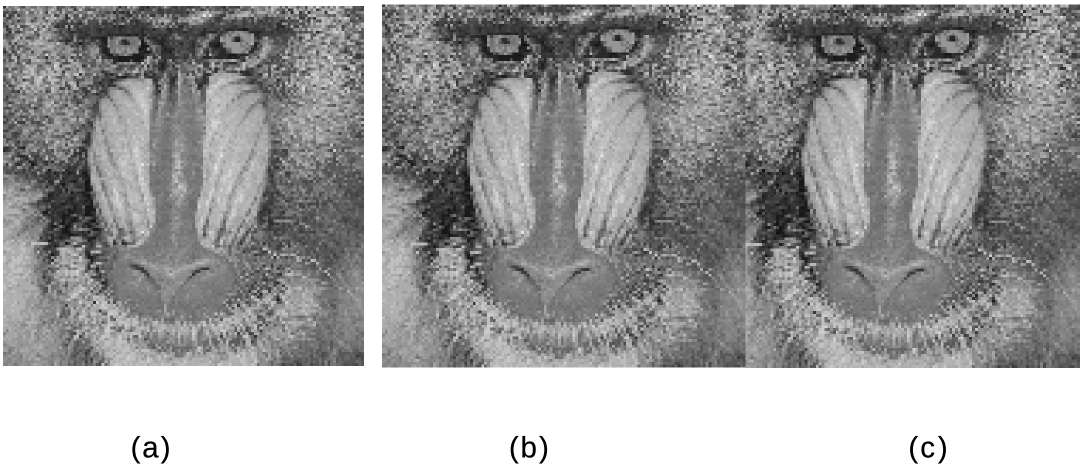


Figure 11. mand image. (a) cover-image, (b) stego-image with seed=5, and (c) stego-image with seed=7.

PDF created with pdfFactory Pro trial version www.pdffactory.com

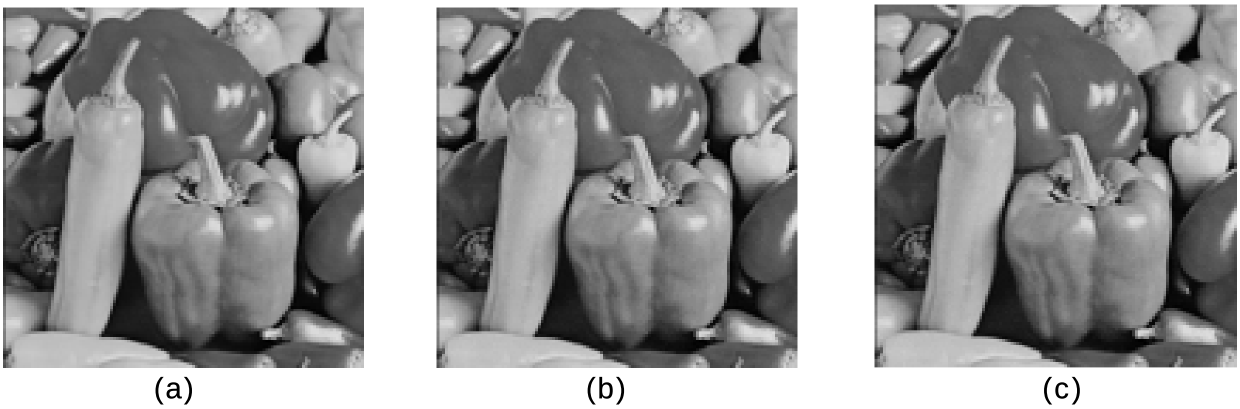


Figure 12. peppers image. (a) cover-image, (b) stego-image with seed=5, and (c) stego-image with seed=7.

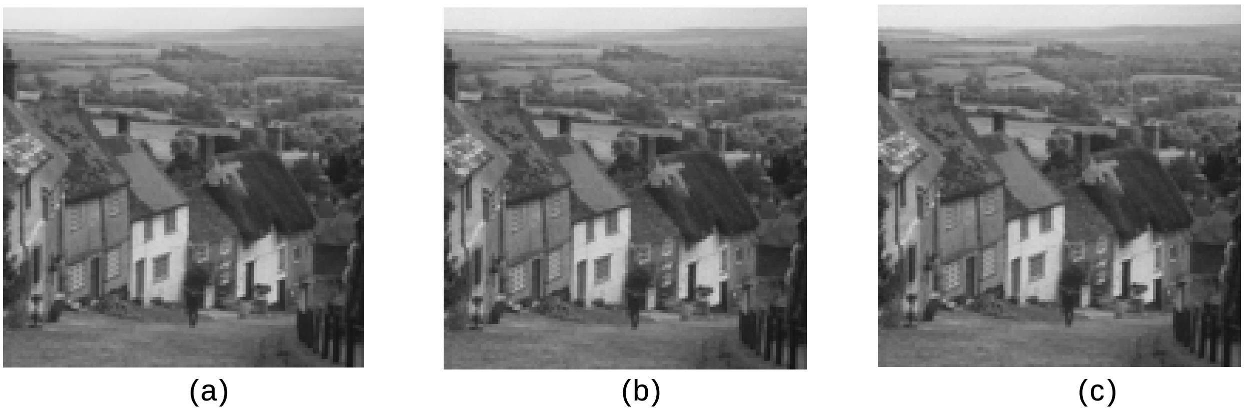


Figure 13. goldhill image. (a) cover-image, (b) stego-image with seed=5, and (c) stego-image with seed=7.

PDF created with pdfFactory Pro trial version www.pdffactory.com