Alustath Journal for Human and Social Sciences

Volume 219 | Issue 1 Article 3

11-15-2016

Domino, novel steganography system

Nadia Mohammed Abdulmajeed
University of Baghdad,College of education for pure since/Ibn-Alhaitham

Recommended Citation
Abdulmajeed, Nadia Mohammed (2016) "Domino, novel steganography system," *Alustath Journal for Human and Social Sciences*: Vol. 219: Iss. 1, Article 3.
DOI: 10.36473/ujhss.v219i1.497
Available at: https://alustath.uobaghdad.edu.iq/journal/vol219/iss1/3

Domino, novel steganography system

Nadia mohammed Abdulmajeed
Teacher, Collage of education for pure since/Ibn-Alhaitham, Baghdad University
MSc of computer science
omrahuma@yahoo.com

Abstract:

Primary objective of the proposed system is to achieve higher level of confidentiality in absence of standard encryption techniques which add up to complexity of the stego system.

In this system the principle of dominoes is adopted in the way of the selection of the pixel of the image to hide the ciphertext. Where domino stones models are prepared in advance, which are two-dimensional matrices (2*6), and selecting one of them and start the projection of the model on the image and hide the ciphertext in the pixel corresponding to the points in the domino model

Experimental results show that the proposed system effectively achieve the objective. Even though the proposed system gives good enhancement to the steganoraphy technique and there is no difference between the cover-image and the stego-image can be seen by the human vision system (HVS), so this method can be considered as a success and can be adopted in the field of steganography.

Keywords: steganography, embedding, extracting, domino.

1. Introduction

Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). However, in the hiding information the meaning of Steganography is hiding text or secret messages into another media file such as image, text, sound, and video. [1][2][7]

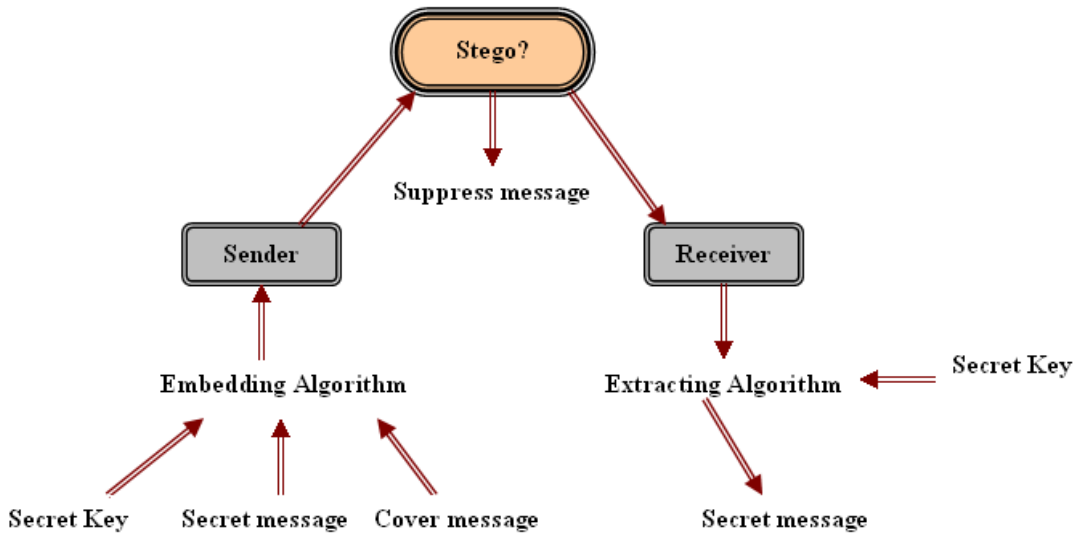
Steganography ancient origins traced back to 440 BC. It was started by the Greeks by shaving the slaves' hair heads and writing the message on their heads, after the hair had been grown, they were sent to their allies in order to communicate with them without the enemies' knowledge [7]. As well as, the invisible ink used for hiding the secret messages by the American revolutionaries during the USA Revolution. Also it was used in both World Wars by German army [8]. Another Steganography technique is the Spam Mimic software which developed by Wayner in (2003), this software was developed to detect and hide the secret messages in text file based on set of protocols [9] [12].

The motivation behind developing image Steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members

of the military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage. The main goal of using the Steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message.[3][4]

The main terminologies used in the Steganography systems are: the cover message, secret message, secret key and embedding algorithm [5]. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to embed the secret information in the cover message.[7][12]

In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which suppose to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender [7][12]. The Steganography system scenario is



shown in the Figure 1.

Figure 1: Steganography System Scenario

Many carrier messages can be used in the recent technologies, such as Image, text video and many others. The image file is the most popular used for this purpose because it easy to send during the communication between the sender and receiver. The images are divided into three types: binary (Black- White), Gray scale and Red-Green-Blue (RGB) images. The binary image has one bit value per pixel represent by 0 for black and 1 for white pixels. While the gray scale image has 8 bits value per pixel represent from 00000000 for black and 11111111 for white pixels. The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels. The RGB image is the most suitable because it contains a lot of information that help in hiding the secret information with a bit change in the image resolution which does not affect the image quality and make the message more secure. In this research paper the RGB images are used as a carrier message to hide the secret messages by the Least Significant Bit hiding method (LSB) as well as the proposed system. [6][5]

2. Image steganography

Image compression techniques are extensively used in steganography. Among the two types of image compressions, lossy compression and loss less compression; lossless compression formats offer more promises. Lossy compression may not maintain the original image's integrity. Lossless compression maintains the original image data exactly, hence it is preferred. Example of lossy compression format is JPEG format files. Examples of Lossless compression formats are GIF [10] and BMP formats.

3. Evaluation Parameters

To measure the image quality, commonly used Mean-Squared Error and Peak Signal-to-Noise Ratio to compare stego-image with cover results [11].

3.1. Mean-Squared Error

The mean-squared error (MSE) between two images *I1 (m, n)* and *I2(m, n)* is [11]:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

M and *N* are the number of rows and columns in the input images, respectively. Mean-squared error strongly depends on the image intensity scaling [11].

3.2. Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) is measured in decibels (dB) avoids this problem by scaling the MSE according to the image range [11]:

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

Where R, is the maximum fluctuation in the input image data type.

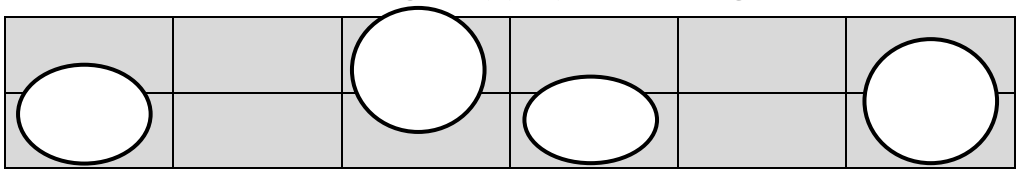
For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc [11].

4. Proposed system

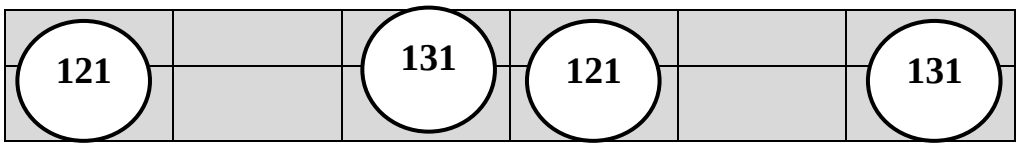
In this system the principle of dominoes is adopted in the way of the selection of the pixel of the image to hide the ciphertext. Where domino stones models are prepared in advance, which are two-dimensional matrices (2*6), and selecting one of them and start the projection of the model on the image and hide the ciphertext in the pixel corresponding to the points in the domino model see figure (2). After selecting the pixels, they will be dismantled to the main colors (Red Green Blue), the matching of the data in 1 or 2 LSBs with the encrypted text data is verified, and the data of each color is replaced with the text data after it's converted to the binary system, and this process is repeated until finishing the domino model which was selected and registered in an index table with the number of points and the location of the used bits of the image to hide, and the right half of the matrix will determine the selection of the following model of the remaining dominoes, this process is repeated until the completion of the entire text is hidden in the image.

123	121	131	123	121	131
121	131	123	121	131	123

Figure (2): a) cover-image.



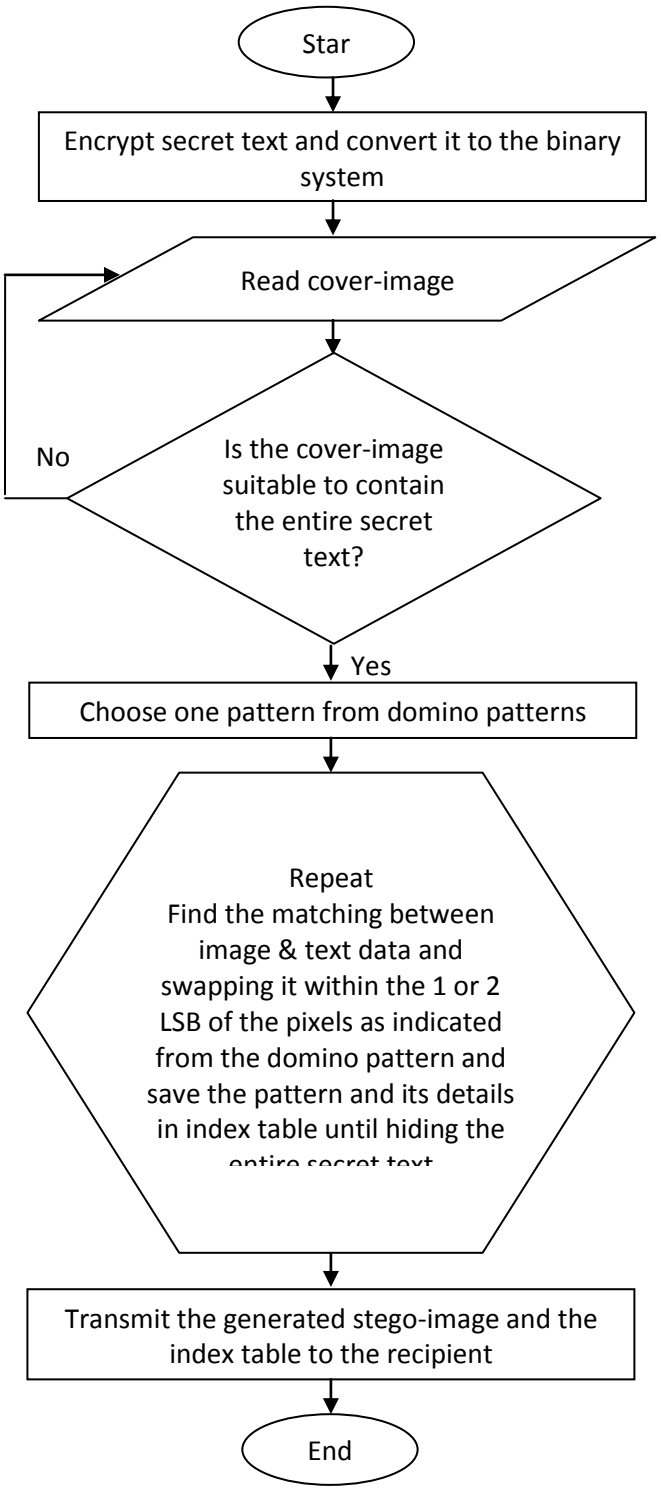
b) Pattern of the domino.



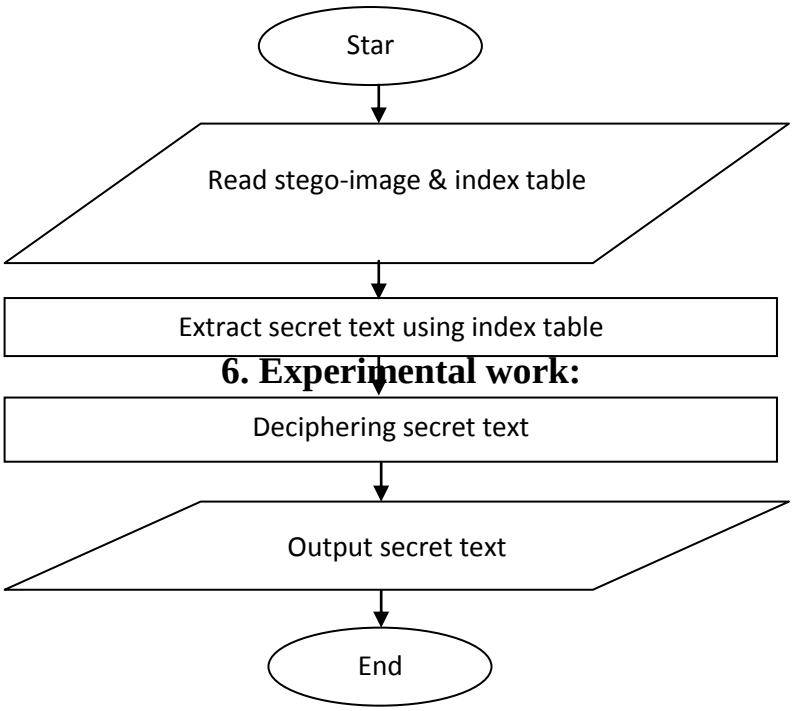
c) stego-image

5. The flowchart of the proposed system:

Embedding operation:



Extracting operation:



6. Experimental work:

Different sizes of a 24 true color cover-images are used. Figure (3) shows the images used in the experiments. The length of the secret text is chooses by two randomization characters lengths 20 and 256.

The stego-images are show in figure (4a, 4b) as a result of the proposed system on the images above.

Figure (3): a) lena cover-image b) mona cover-image

Figure (4): a) lena stego-image b) mona stego-image

7. Experimental results:

The evaluation parameters MSE and PSNR are used to verify the image quality between cover-image and stego-image in experiments which varied depending on the variation of many factors effects the performance of the proposed system such as the size of the cover-image and the length of the secret text.

Following table shows the result of the proposed system for the images above:

Image name	Lena.jpg 24 true color	mona.jpg 24 true color
Image size	512 x 512	256 x 256
Message (no. of char.)	250	20
PSNR of stego-image	70.8769	79.4832
MSE of stego-image	0.0612	8.70E-04

From above table it can be seen that the quality of the cover image affected by increasing the length of the secret text. The PSNR is decreases (lower quality) by increasing the secret text length and the MSE is increases and vice versa. This is due to the increasing of the number of pixels in cover image that will change such that the distortion is increases and the quality is decreases.

8. Conclusion

Experimental results show that the proposed system effectively achieve the objective. Even though the proposed system gives good enhancement to the steganoraphy technique and there is no difference between the cover-image and the stego-image can be seen by the human vision system (HVS), so this method can be considered as a success and can be adopted in the field of steganography.

The Implementation of this method for Audio and Video Steganography will considered as a future work.

References:

[1] B. Dunbar. A detailed look at Steganographic Techniques and their use in annOpen-Systems Environment, Sans Institute, 1(2002).
[2] C. Christian. An Information-Theoretic Model for Steganography, Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science. 1998.
[3] H. Wu, H. Wang, C. Tsai and C. Wang, Reversible image steganographic scheme via predictive coding. 1 (2010), ISSN: 01419382, 35-43.
[4] J, Corporation, Steganography.
http://www.webopedia.com/TERM/S/steganography.html. 2005.
[5] Jessica Fridrich, Miroslav Goljan, and Rui Du., "Detecting LSB Steganography in Color and Gray- Scale Images", - IEEE Multimedia.
[6] N Ghoshal, J K Mandal .A steganographic scheme for colour image authentication (SSCIA), Recent Trends in Information Technology ICRTIT 2011 International Conference on (2011), 826-831.
[7] N. Johnson, Survey of Steganography Software, Technical Report, January 2002.
[8] P. Fabien, J. Ross. Anderson, and Markus G. Kuhn. "Information Hiding – A Survey." Proceedings of the IEEE, 87:7. 1062-1078. 1999.
[9] Spam Mimic." http://www.spammimic.com.
[10] T. Moerland, "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001 Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999.
[11] V. Lokeswara Reddy, Dr. A. Subramanyam, and Dr.P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications Volume: 02, Issue: 05, Pages: 868-872, 2011
[12] W, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking (second edition). San Francisco: Morgan Kaufmann. 3(1992) 192-213.

الدومينو نظام إخفاء المعلومات الرواية

م.م. نادية محمد عبد المجيد
جامعة بغداد/ كلية التربية للعلوم الصرفة/ ابن الهيثم

الملخص:

الهدف الرئيس من النظام المقترح هو تحقيق مستوى أعلى من السرية في غياب تقنيات التشفير القياسية التي تضيف تعقيد أكثر لنظام إخفاء المعلومات. في هذا النظام يتم اعتماد مبدأ لعبة الدومينو في طريقة انتقاء البكسل من الصورة لإخفاء النص المشفر فيها. حيث تُجهز نماذج أحجار لعبة الدومينو بشكل مسبق والتي تكون عبارة عن مصفوفات ثنائية الأبعاد (٢×٦) ويتم انتقاء إحداها والبدء بتسقيط النموذج على الصورة وإخفاء النص المشفر في البكسل المقابلة للنقاط الموجودة في نموذج حجر الدومينو. وقد أظهرت النتائج أن النظام المقترح حقق الهدف بفعالية. على الرغم من أن النظام المقترح يعطي تعزيز جيد لتقنية إخفاء المعلومات وليس هناك فرق بين الصورة الغطاء والصورة الناتجة يمكن أن يُرى من قبل نظام رؤية الإنسان، لذلك هذه الطريقة يمكن اعتبارها ناجحة، ويمكن اعتمادها في مجال إخفاء المعلومات.

الكلمات المفتاحية: إخفاء المعلومات، التضمين، واستخراج، الدومينو.