A Proposal of Steganography Algorithm by Random Image Transformation

Maisa'a Abid Ali Kodher
Maisaa_ali2013@uotechnology.edu.iq
University of Technology
Department of Computer Sciences
Baghdad - Iraq

Abstract: *The rapid developments in communications systems and the Internet have led to propose a new hiding algorithm to transfer the image, text, or voice over the Internet and network. The image is considered a cover to hide the massage by using a secret random key. The secret key is 9×9 matrix and then random elements are selected to make inverse matrix. The inverse matrix is multiplied by one–dimensional matrix, resulting in hidden images. This algorithm keeps the images secret during transmission through network. Such a process is known as random image transformation and is regarded as a reliable means of concealment.*

The results obtained from the proposed algorithm depend on the cover image. The secret key is generated so that it can restore the original image *after receiving without losing of any hidden information by recipient in the network.*

Key words: Steganography, Transform dynamic random image, Random matrix, Inverse matrix, Secret key.

1. Introduction

During the last decade, Internet activities have become an important part of many people's lives. As the number of these activities increases, there is a growing amount of personal information about the users that is stored in electronic form and that is usually transferred using public electronic means. This makes it feasible and often easy to collect, transfer and process a huge amount of information about person. As a consequence, the need for, mechanism to protect such information is compelling [1]. The growing possibilities of modern communications need special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity need to the processed in protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding [2].

Steganography is a technique of hiding information in digital media. The goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas [2]. Digital audio, video, and image are increasingly furnished with distinguishing but imperceptible marks, which may contain a hiding copyright notice or serial number or even help to prevent unauthorized copying directly. This approach of information hiding can be extended to copyright protection for digital media: audio, video, and images. The information hiding includes cover channels, steganography (linguistic steganography and technical steganography), anonymity, and copyright marking.

The technical steganography consists of: substitutions of system, masking and filtering, transformation domain, spread spectrum technique, distortion technique, statistical methods, and cover generating methods [3].

2. Steganography

Steganography is the science of hiding information by embedding the hidden (secret) message within a cover media such as an image, audio, and video carrier file in such a way that the hidden information cannot be easily perceived to exist for the unintended recipients of the cover media [4],[5]. Steganography hiding model takes advantage of the redundancy of data such that there could be no perceptible change to the cover media see Fig. (1).

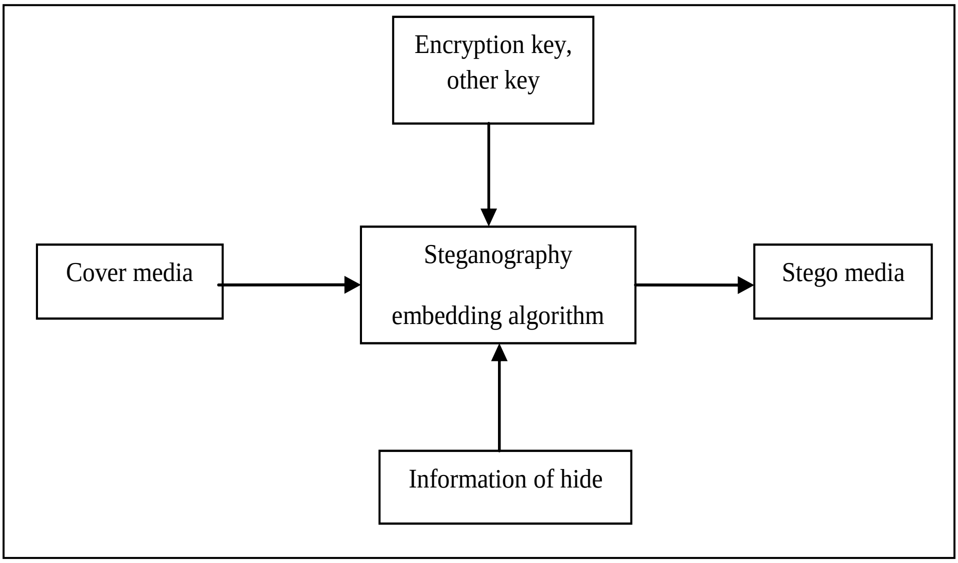


Fig. (1) Hiding Model

In the steganography extraction model, the extraction process should be possible without the cover; the extraction algorithm can also be applied to any cover, whether or not it contains a secret message. In the latter case, the output of the extraction process is considered as a "natural randomness" of the cover [4] [5], see Fig. (2).

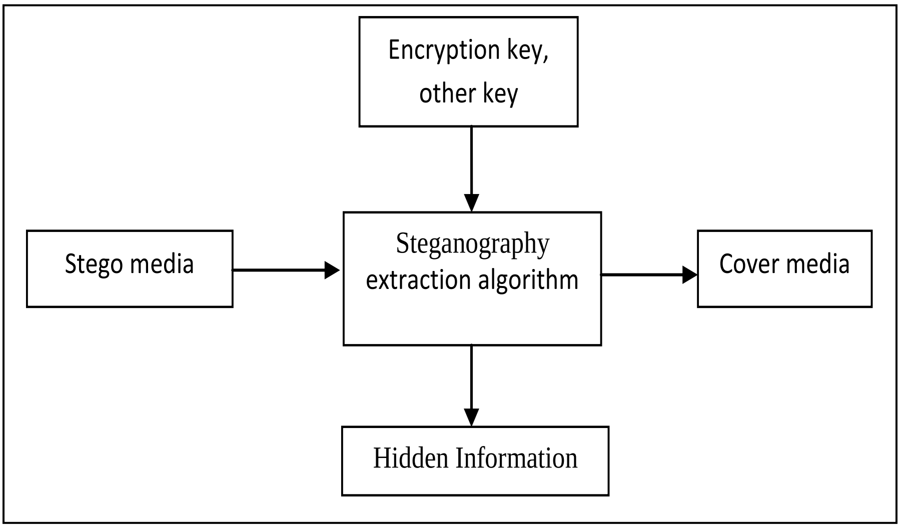


Fig. (2) Extraction Model

3. Steganography Types

As it is known there is much communication between people and organizations through the use of phone, the fax, computer communications, radio, and of course all of these communications should be secure. There are basically three Steganography types [6].

1. Pure Steganography.
2. Secret key Steganography.
3. Public key Steganography.

3.1 Pure Key Steganography:

Pure steganography is a steganography system that doesn't require prior exchange of some secret information before sending message; therefore, no process: the security of the system thus depends entirely on its secrecy [3] [7].

The pure steganography can be defined as the quadruple (C, M, D, and E) where:

C: the set of possible covers.
M: the set of secret massage with |C| ≥ |M|.
E: C*M→C the embedding function.

D: C→M of the extraction function with the property that D (E(c, m)) = m

for all m Є M and c Є C see Fig. (3).

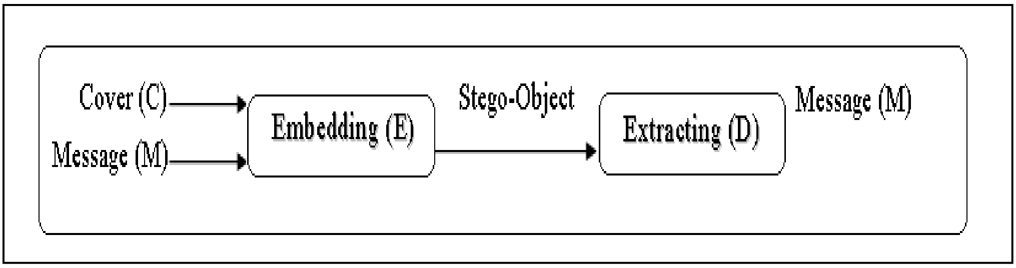


Fig. (3) Pure Key Steganography

3.2 Secret Key Steganography:

A secret key steganography system is similar to asymmetric cipher, where the sender chooses a cover and embeds the secret message into the cover using a secret key. If the secret key used in the embedding process is known to the receiver, he/she can reverse the process and extract the secret message [7]. Anyone who doesn't know the secret key should not be able to obtain evidence of the encoded information [3] [6] [7].

The secret key steganography can be defined as the quintuple (C, M, K, DK, EK) where:
C: the set of possible covers.
M: the set of secret message.
K: the set of secret keys.
Ek: C×M×K→C

With the property that DK (EK(c,m,k),k)=m for all m ЄM, c Є C and k Є K , see Fig. (4).

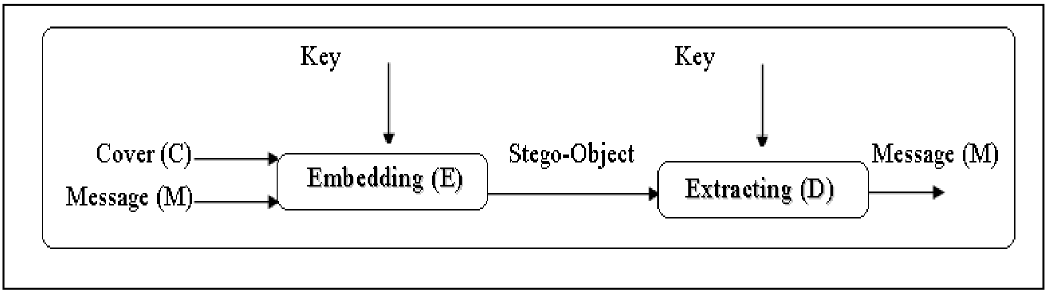


Fig. (4) Secret Key Steganography.

3.3 Public Key Steganography:

Public key Steganography does not depend on the exchange of a secret key. It requires two keys, one of them private (secret) and the other public: the public key is stored in a public database, whereas the public key is used in the embedding process. The secret key is used to reconstruct the secret message.

One way to build a public key Steganography system is to use a public key cryptosystem. The sender and the receiver can exchange public keys of some public key cryptography algorithm before imprisonment. Public key Steganography utilizes the fact that the decoding function in a Steganography system can be applied to any cover, whether or not it already contains a secret message.

The public key Steganography relies on the fact that encrypted information is random enough to hide in plain sight. The sender encrypts the information with the receiver's public key to obtain a random-looking massage and embeds it in a channel known to the receiver, thereby replacing some of the natural randomness with which every communication process is accompanied. Assume that both the cryptographic algorithms and the embedding functions are publicly known [7].

4. Image Steganography

Images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithm exists. An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms grid and the individual points are referred to as pixels. Most images on the internet consist of a rectangular map of the image's pixels (represented as bits) where each pixel is located with its color. These pixels are displayed horizontally row by row [8], [9].

5. Proposed Random Hiding Algorithm

```
Process:
Input:  Original image.
Output: Stego image.
Initial:
        A = Load Original Image 96×96.
        B = Execute Block Image 32×32.
        C = Execute Random Image (Cover Image) 1-D.
        D =Load Inverse Matrix randomize (Key Secret) 9×9.
        E = Stego Image 1-D.
Step 1: Divide Original Image 32×32 Equal 9 Blocks of Original
        Image in B.
Step 2: Find Cover Image From Elements of Matrix One
        Dimension Random From Each Block of Image in C.
Step 3: Select Elements of Matrix 9×9 and Randomize.
Step 4: Find Determent of Matrix 9×9 Randomize.
Step 5: Find Secret Key From Inverse Matrix in D.
Step 5: Multiply 1-D Cover Image with Inverse Matrix.
Step 6: Result (Put the result of Stego Image 1-D in E).
```

5.1 Random Hiding Algorithm

- **This algorithm consists of four steps:**

The First Steps:

The original image is used as a cover image, Fig. (5) shows an example of cover image. It is divided into nine blocks each of which has dimension of 32 pixels as shown in Fig. (6-a,b). After image division, random points are taken from the image using dynamic random generating function. The function takes random points from the image every time, that is, it takes nine points from each block, these points have color value of the original image consisting of (X,Y). X and Y have values in RGB range. These random points generate one–dimensional matrix as shown in Fig. (6-c).

Fig. (5) Original Image 96×96

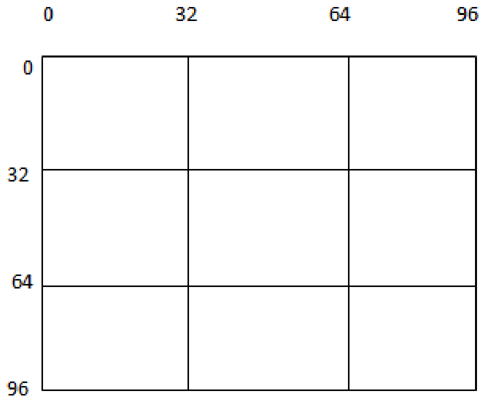


Fig. (6-a) Partition Image into Nine Block of Size 32×32

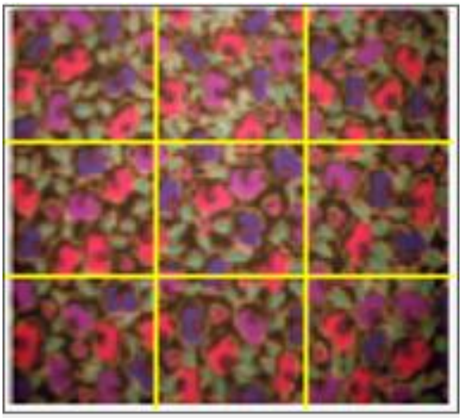


Fig. (6-b) Edge Partition Image into Nine Block of Size 32×32

Random point of original image X=RGB, Y=RGB

Random point matrix one – dimension

RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB
X1,Y1	X2,Y2	X3,Y3	X4,Y4	X5,Y5	X6,Y6	X7,Y7	X8,Y8	X9,Y9

Suppose the values of random value are:

RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB
23,1	57,21	85,8	7,57	34,52	82,91	76,16	78,55	79,74

Fig. (6-c) Image Random Points

The Second step:

A secret key is generated to hide the original image. The secret key elements are randomly selected from 9×9 matrixes. The determinate is obtained from random matrix. Then the inverse random matrix is calculated and multiplied by one-dimensional image.

The inverse matrix is considered the secret key to hide the colored image. Thus colored images get hiding in one-dimensional matrix. Each value has red, green, and blue colors, as shown in Figs. (7 and 8). The hidden image can be transmitted across network and internet.

- Random matrix 9×9:

$$\begin{bmatrix} 0.8147 & 0.9649 & 0.7922 & 0.3922 & 0.6948 & 0.4898 & 0.1190 & 0.6991 & 0.8143 \\ 0.9058 & 0.1576 & 0.9595 & 0.6555 & 0.3171 & 0.4456 & 0.4984 & 0.8909 & 0.2435 \\ 0.1270 & 0.9706 & 0.6557 & 0.1712 & 0.9502 & 0.6463 & 0.9597 & 0.9593 & 0.9293 \\ 0.9134 & 0.9572 & 0.0357 & 0.7060 & 0.0344 & 0.7094 & 0.3404 & 0.5472 & 0.3500 \\ 0.6324 & 0.4854 & 0.8491 & 0.0318 & 0.4387 & 0.7547 & 0.5853 & 0.1386 & 0.1966 \\ 0.0975 & 0.8003 & 0.9340 & 0.2769 & 0.3816 & 0.2760 & 0.2238 & 0.1493 & 0.2511 \\ 0.2785 & 0.1419 & 0.6787 & 0.0462 & 0.7655 & 0.6797 & 0.7513 & 0.2575 & 0.6160 \\ 0.5469 & 0.4218 & 0.7577 & 0.0971 & 0.7952 & 0.6551 & 0.2551 & 0.8407 & 0.4733 \\ 0.9575 & 0.9157 & 0.7431 & 0.8235 & 0.1869 & 0.1626 & 0.5060 & 0.2543 & 0.3517 \end{bmatrix}$$

Fig. (7) Random Matrix

- Determine the determinate of random matrix:

Multiply elements of head diameter - multiply elements of secondary diameter = -0.0394

Divide determinate value of all the elements of a random matrix.

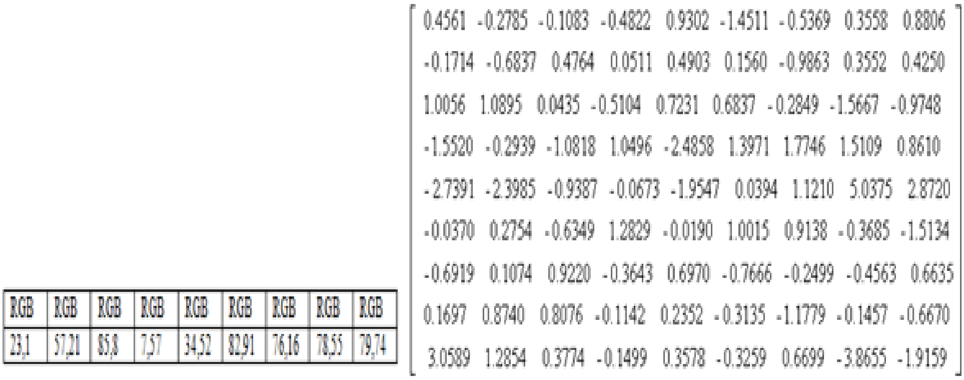
- Find inverse matrix (secret key):

$$\begin{bmatrix}
0.4561 & -0.2785 & -0.1083 & -0.4822 & 0.9302 & -1.4511 & -0.5369 & 0.3558 & 0.8806 \\
-0.1714 & -0.6837 & 0.4764 & 0.0511 & 0.4903 & 0.1560 & -0.9863 & 0.3552 & 0.4250 \\
1.0056 & 1.0895 & 0.0435 & -0.5104 & 0.7231 & 0.6837 & -0.2849 & -1.5667 & -0.9748 \\
-1.5520 & -0.2939 & -1.0818 & 1.0496 & -2.4858 & 1.3971 & 1.7746 & 1.5109 & 0.8610 \\
-2.7391 & -2.3985 & -0.9387 & -0.0673 & -1.9547 & 0.0394 & 1.1210 & 5.0375 & 2.8720 \\
-0.0370 & 0.2754 & -0.6349 & 1.2829 & -0.0190 & 1.0015 & 0.9138 & -0.3685 & -1.5134 \\
-0.6919 & 0.1074 & 0.9220 & -0.3643 & 0.6970 & -0.7666 & -0.2499 & -0.4563 & 0.6635 \\
0.1697 & 0.8740 & 0.8076 & -0.1142 & 0.2352 & -0.3135 & -1.1779 & -0.1457 & -0.6670 \\
3.0589 & 1.2854 & 0.3774 & -0.1499 & 0.3578 & -0.3259 & 0.6699 & -3.8655 & -1.9159
\end{bmatrix}$$

Fig. (8) Inverse Random Matrix

The Third step:

- Multiplication of the one dimension random point matrix in step 1 with random inverse matrix in step 2.



RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB
23,1	57,21	85,8	7,57	34,52	82,91	76,16	78,55	79,74

$$\begin{bmatrix}
0.4561 & -0.2785 & -0.1083 & -0.4822 & 0.9302 & -1.4511 & -0.5369 & 0.3558 & 0.8806 \\
-0.1714 & -0.6837 & 0.4764 & 0.0511 & 0.4903 & 0.1560 & -0.9863 & 0.3552 & 0.4250 \\
1.0056 & 1.0895 & 0.0435 & -0.5104 & 0.7231 & 0.6837 & -0.2849 & -1.5667 & -0.9748 \\
-1.5520 & -0.2939 & -1.0818 & 1.0496 & -2.4858 & 1.3971 & 1.7746 & 1.5109 & 0.8610 \\
-2.7391 & -2.3985 & -0.9387 & -0.0673 & -1.9547 & 0.0394 & 1.1210 & 5.0375 & 2.8720 \\
-0.0370 & 0.2754 & -0.6349 & 1.2829 & -0.0190 & 1.0015 & 0.9138 & -0.3685 & -1.5134 \\
-0.6919 & 0.1074 & 0.9220 & -0.3643 & 0.6970 & -0.7666 & -0.2499 & -0.4563 & 0.6635 \\
0.1697 & 0.8740 & 0.8076 & -0.1142 & 0.2352 & -0.3135 & -1.1779 & -0.1457 & -0.6670 \\
3.0589 & 1.2854 & 0.3774 & -0.1499 & 0.3578 & -0.3259 & 0.6699 & -3.8655 & -1.9159
\end{bmatrix}$$

- The result is stego image with one – dimensional matrix.

RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB
27.17.24	19.18.14	31.26.17	143.42.70	109.70.36	132.77.41	25.17.12	48.18.15	50.14.22

The Fourth step:

Transformation of original 96×96 image to stego image uses function which multiplies random cover by inverse matrix as shown in Fig. (9-a,b).

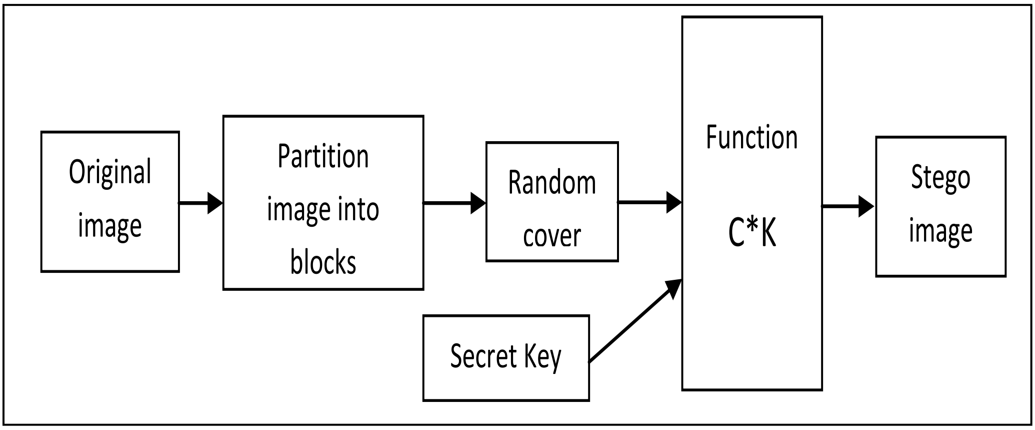
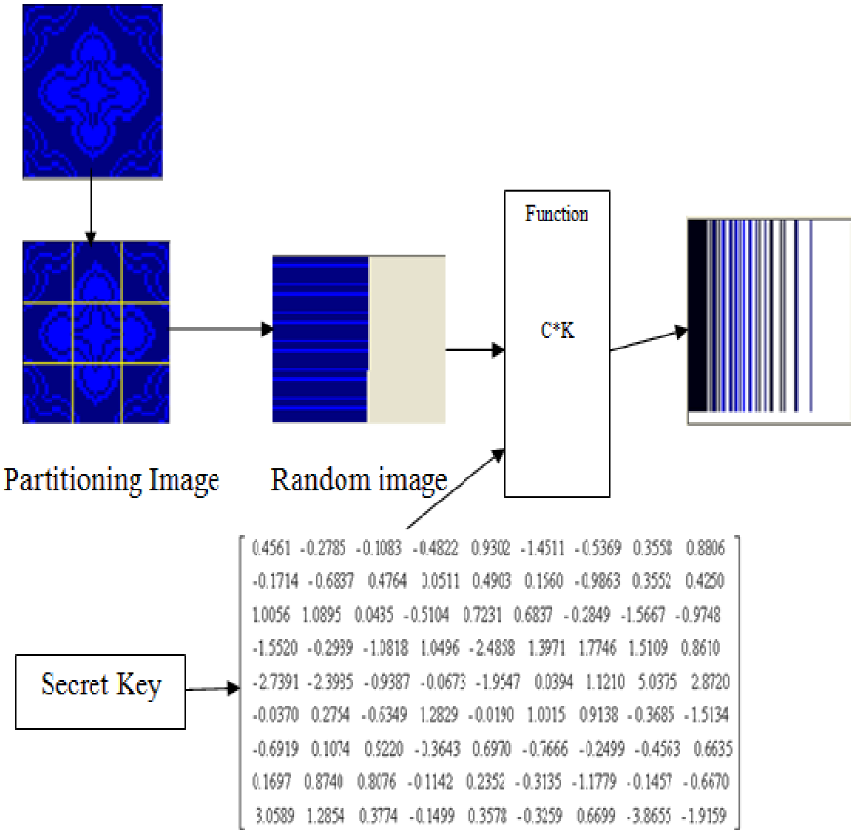


Fig. (9- a) Transform Original Image to Stego Image

Example:

Original Image

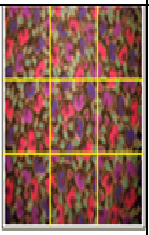
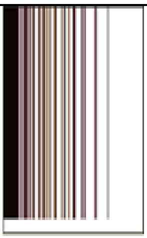
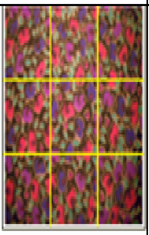
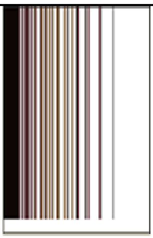
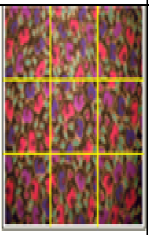
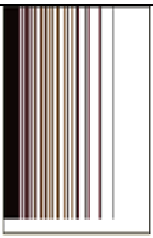


$$\begin{bmatrix} 0.4561 & -0.2785 & -0.1083 & -0.4822 & 0.9302 & -1.4511 & -0.5369 & 0.3558 & 0.8806 \\ -0.1714 & -0.6837 & 0.4764 & 0.0511 & 0.4903 & 0.1560 & -0.9863 & 0.3552 & 0.4250 \\ 1.0056 & 1.0895 & 0.0435 & -0.5104 & 0.7231 & 0.6837 & -0.2849 & -1.5667 & -0.9748 \\ -1.5520 & -0.2939 & -1.0818 & 1.0496 & -2.4858 & 1.3971 & 1.7746 & 1.5109 & 0.8610 \\ -2.7391 & -2.3935 & -0.9387 & -0.0673 & -1.9547 & 0.0394 & 1.1210 & 5.0375 & 2.8720 \\ -0.0370 & 0.2754 & -0.6349 & 1.2829 & -0.0190 & 1.0015 & 0.9138 & -0.3685 & -1.5134 \\ -0.6919 & 0.1074 & 0.5220 & -1.3643 & 0.6970 & -0.7666 & -0.2499 & -0.4563 & 0.6635 \\ 0.1697 & 0.8740 & 0.8076 & -0.1142 & 0.2352 & -0.3135 & -1.1779 & -0.1457 & -0.6670 \\ 3.0589 & 1.2854 & 0.3774 & -0.1499 & 0.3578 & -0.3259 & 0.6699 & -3.8655 & -1.9159 \end{bmatrix}$$

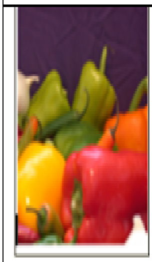
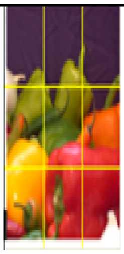
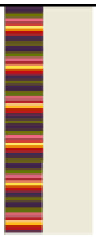
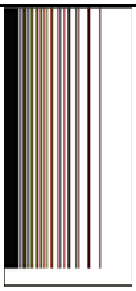
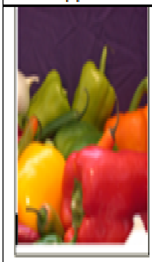
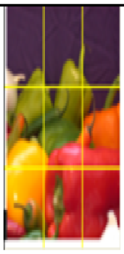
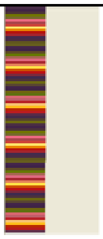
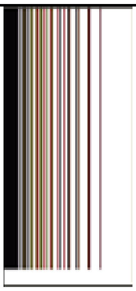
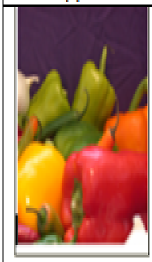
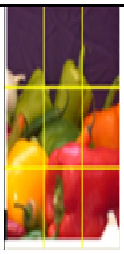
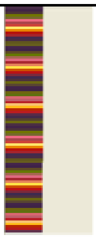
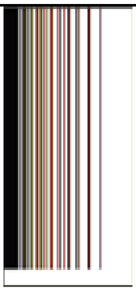
Fig. (9- b) Transform Original Image to Stego Image

5.2 Result of Test

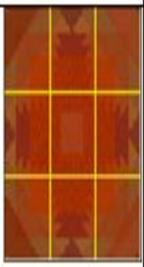
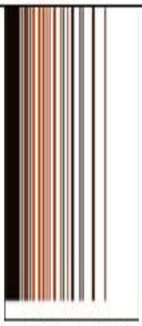
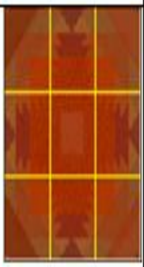
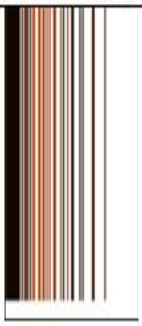
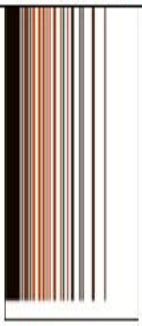
Test 1: fabric image:

Original Image 96X96	Block Image 96X96	Random Image 1-D X,Y	RGB	RGB	INV Matrix Found in fig.(8)	Stego Image	RGB
			X	Y			1-D Stego Image
 Fabric1			24 53 93 20 80 92 81 94	26 17 4 48 68 8 35 93	[illegible]	 PSNR=1.3269	46.17.20 13.9.10 20.22.13 249.67.91 248.248.0 127.99.66 9.5.4 24.15.9 27.17.26
 Fabric2			1 40 71 11 55 73 95 78 94	81 11 11 45 33 79 25 39 89	[illegible]	 PSNR=1.2471	42.35.33 11.7.7 26.17.10 68.44.22 153.99.72 200.42.59 35.35.35 26.18.11 25.15.19
 Fabric3			7 59 89 22 60 73 66 86 81	16 17 0 50 64 81 20 61 72	[illegible]	 PSNR=1.2193	38.17.13 18.12.7 34.35.33 153.132.104 284.284.0 175.73.56 29.10.12 12.8.7 69.37.30

Test 2: pepper image

Original Image 96X96	Block Image 96X96	Random Image	RGB	RGB	INV Matrix Found in fig.(8)	Stego Image	RGB
			X	Y			1-D Stego Image
 Pepper1			14 37 72 20 33 67 63 63 78	22 2 27 44 50 88 30 40 79	[illegible]	 PSNR=1.2024	17.10.17 8.4.8 13.7.12 168.159.29 112.123.24 168.33.38 20.18.0 38.29.2 83.6.14
 Pepper2			24 42 91 5 48 87 67 69 95	19 14 29 39 38 81 29 49 80	[illegible]	 PSNR=1.3699	17.10.16 8.5.8 17.15.10 211.172.131 150.140.28 159.113.123 14.12.4 43.29.20 63.10.18
 Pepper3			8 54 76 27 46 95 91 88 68	13 10 10 33 34 70 20 37 83	[illegible]	 PSNR=1.2501	17.10.17 8.5.8 14.8.14 188.183.28 136.132.20 153.20.33 9.5.9 36.30.4 91.21.25

Test 3: zapotac image:

Original Image 96X96	Block Image 96X96	Random Image	RGB	RGB	INV Matrix Found in fig.(8)	Stego Image	RGB
			X	Y			1-D Stego Image
 Zapotac1			10 55 64 22 47 84 85 65 91	9 15 21 60 38 68 24 62 71	[illegible]	 PSNR=1.0784	31.13.4 16.5.2 53.53.0 204.67.0 160.40.0 141.59.22 21.9.3 52.14.0 71.42.17
 Zapotac2			21 31 75 19 33 70 76 91 81	4 27 27 34 33 85 20 57 70	[illegible]	 PSNR=1.5202	33.17.8 19.6.0 36.12.2 204.67.9 160.55.8 133.59.22 23.8.1 52.30.14 75.34.12
 Zapotac3			21 43 81 27 64 69 72 80 90	10 5 1 43 61 68 9 37 68	[illegible]	 PSNR=1.5548	35.15.6 14.6.4 31.14.7 195.48.0 248.248.0 156.51.7 19.11.6 46.14.8 71.38.17

6. Conclusion

This research provides a good and efficient method for steganography of image by reducing image size for transmitting it to the destination across network and internet in a secure way.

In this system, the image data is of static size. The system transforms the image to a set of blocks of images. It randomly selects coordinates of image pixels at a dynamic random image; it becomes a suitable cover for a small-sized image.

On stego image examination by using PSNR, it is found that the values of PSNR vary with dynamically random points, thus increasing the hiding image efficiently.

The value of PSNR ranges from 1.2 to 1.3 or 1.0 to 1.5, in a way that these ranges give robustness to the hidden image.

The steganography technique in this research is robust to hide image across network depending on dynamic random and secret key. In random transform technique compared with discrete cosine transform (DCT) and discrete wavelet transform (DWT) the original image can be restored whereas in DCT and DWT original image cannot be restored completely.

References

[1] R. Beauxis1, et al., "Formal Approaches to Information Hiding", 2008. Available at: vanilla47.com/steganography/AN%20 overview%20 of %20 IMAG.

[2] M. M. Amin, et al., "Information Hiding Using Steganography", 4th National Conference On Telecommunication Technology Proceedings (NCTT2003), Shah Alam, Malaysia, pp.21-25, January 14-15, 2003.

[3] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding A Survey", Proceeding of the IEEE, Special Issue on Protection of Multimedia content, 87 (7):1062- 1078, July 1999.

[4] Natarajan Meghanathan, "Basics of Steganography and Security of Steganography Systems", Jackson state university, Jackson MS 39217, 2005. Available at: natarajan.meghanathan@jsums.edu.

[5] Eric Cole, Ronald D. Krutz, " Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley Publishing, Inc., 2003.

[6] Z. Kh. AL-Ani, A.A. Zaidan, B.B. Zaidan and H.O.Alanazi, "Main Fundamentals for Steganography" Journal of Computing, Vol. 2, Issue 3, March 2010.

[7] H.A.Jalab, A.A Zaidan, B.B Zaidan, "New Design for Information Hiding With in Steganography Using Distortion Techniques", International Journal of Engineering and Technology (IJET)), Vol. 2, No. 1, Feb (2010).

[8] R. Yadav, U.I.E.T, M.D.U,Rohtak, "Study of information Hiding Techniques and their Counterattacks: A Review Article", International Journal of Computer Science & Communication Network, Vol 1(2), 2011.

[9] T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of Image Steganography", Information and Computer Security

Architecture (ICSA) Research group Department of Computer Science, University of Pretoria, 2002.

اقتراح خوارزمية اخفاء بالاعتماد على التحويل العشوائي للصورة

م. ميساء عبدعلي خضر
Maisaa_ali2013@uotechnology.edu.iq
الجامعة التكنولوجية - قسم علوم الحاسوب

المستخلص

ان التطورات السريعة في انظمة الاتصالات وشبكات الانترنيت ادت الى اقتراح خوارزمية اخفاء جديدة لنقل الصورة عبر شبكات الانترنيت وتعتبر الصورة غطاء لاخفاء صوت او نص او صورة مع استخدام مفتاح عشوائي سري. تم اختيار عناصر المفتاح السري بشكل مصفوفة عشوائية معكوسة 9×9 والتي تعالج مع الصورة الاصلية وهي ذات بعد واحد ليكونان غطاء الاخفاء. ويمكن استعادة الصورة الاصلية والمعلومة المخفية باستخدام المفتاح السري. نحصل على الصورة المخفية وهذه الخوارزمية تحافظ على سرية الصورة المنقولة عبر الشبكات صورة بصورة آمنة ان هذه الطريقة تسمى التحويل العشوائي في الصورة، وتعتبر وسيلة الإخفاء.

النتائج التي تم الحصول عليها في هذه الخوارزمية المقترحة تعتمد على الصورة الغطاء وعشوائية المفتاح السري المتولد والتي اثبتت عدم ضياع اي من المعلومات المخفية.

الكلمات الرئيسية: الاخفاء، التحويل الديناميكي العشوائي للصورة، المصفوفة العشوائية، المصفوفة المعكوسة، المفتاح السري.