Text Hiding Using Text-Based Captcha Cover Image With Random Method

Zainab Nadhim Adnan, Dr. Jamal M. Kadhim

Republic of Iraq Ministry of Higher Education And Scientific Research Al-Nahrain University College of Science Department of Computer Science

Supervisor

Abstract:

Information Concealment is a task which facing difficult challenges today. This is due to the quick development of concealed information detection methods. The researchers, therefore turned their attention to the development of concealment information methods, become hard for the attackers to get secret information, like introducing a complex algorithm, using randomized methods, and inventing more challenging and complex steps. In this article introduced a new approach of concealment the information in the image. creates new series of challenging stages and mysterious through random bit distribution and the use of the encryption method. Then use the LSB technique to mask the bits within the image. The LSB technique was designed for making it harder to hiding the pixel. The presented results demonstrate the method' s robustness, safety and offer best protection for concealed information. Results displays the accuracy of stego image relative to original image by using the MSE and PSNR quality measurements.

DOI: 10.24297/j.cims.2023.07.13

1. Introduction

The transmission of the the confidential data through internet networks has become a major challenge with the whole development that happened in information technology. Recently, confidential data may be supplied by various methods of data concealment. Cryptography, watermarking, and steganography are the three common ways for information hiding, hiding the message' s existence, and the other ways conceal information such as media format like images, audios, videos, and texts therefore that the other people don' t notice the information' s existence in the above format. lastly, watermark means protecting copyright. Recently, approaches to hide information have given noticeable attention to watermarking and steganography techniques [7]. Steganography is the on of most effective methods of secure communication. Steganography hides all private information in a cover object that looks innocent. The aim, in this paper, is to develop a steganography approach that not just hides the message inside cover image, but it also offers better safety than other methods [1], [2]. steganography techniques conceal the message existence, making it difficult to discovered from a third party [1].

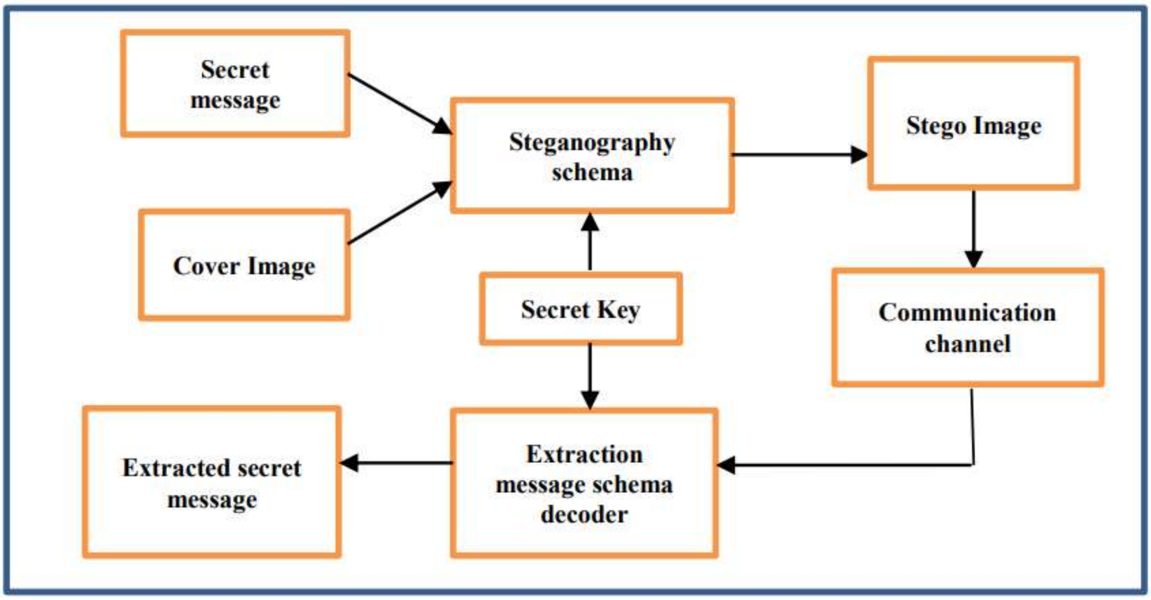


Figure 1. Basic concepts and behavior of steganography

In the steganography of image, the secret message is hidden just in image. Recently, steganography is mainly used with computers, the digital data become media and the networks is become the fast transport channels [3]. Figure1, shows the customary behavior and a key concept in steganography. Steganography technique includes the basic steps that Concealing and retrieving information. Concealing step, is the secret text hiding stage, the secret message that will be embedding in locations that selected in the cover image this selected location based on the appropriate steganography technique. The resultant stego image was sent to the recipient. In the extraction step, the receptor applies the function of extraction to recover the secret message [11]. The cryptography focuses on maintaining the content of message mystery, stenography focuses on maintaining a mystery message presentence [3], [4]. The resultant image is known as stego image, which looks like the cover image. The stego image after that sent to the receptor where the receptor recovers hidden message through the implementation of the process of de-steganography. The embedding process is used stego-key aimed at limiting extraction or unraveling of the message which embedded in the cover media [5].

The stego key is dependent on the randomized generation hidden in a cover image using LSB technique and send the image to the receptor to extract key and in the same sequence to retrieve the message which hidden in the image and this message is embedded also in the same cover image that hidden stego key using the LSB technique. LeastSignificant-Bit (LSB) is the one of the most widely steganography techniques for hiding a mysterious message inside a digital medium. [6].

The recommended method in the paper was the random key generator method, and this for the improvement the security and strength of the steganography technique. In the cover image, the generator of random number locates the hidden column positions in each row separately.

2. Related Work

In the area of steganography, there are a lot of researchers using a method of generating random numbers, and this method marge with another technique and that for hiding the information into the image. Awad A. and Obaida M. proposed the bits of secret message are inserted randomly in the pixels of cover image. The secret text bit' s inserting in the cover image that take place at any bit in the pixel and randomly that is by comparing the bit of pixel with the bit of message that randomly chosen from the 2nd to the last bit. One will be the less significant bit if the compared result is identical, and zero will be the less significant bit if the result isn' t identical. Due to the complexity of the text' s insertion process with the image, therefore attacker can' t retrieve the original text without knowing the positions of the bit and value of PK1 to configured random number using algorithm of RC6 and method of insertion process. Cover image that used is 400*500 and the message to hide was 1KB, resulted PSNR value of stego image was 20.2536dB [3].

Babita el al proposed used the method of random key generation using XOR method for encoding the secret text, and then integrate the encrypted message to RGB image in a special scheme. The resulant image motated to a bitmap format file [8]. Balvinder el al. using XOR method of encryption for encrypting the secret text using 8bits random key. After that, applied XOR method between the 2nd LSB of the pixel of cover image and one bit of 8bits random key. If the result of XOR of the above is 1, therefore one bit in the secret key was hidden in LSB of the same pixel in the cover image. Else, nothing to hide in this pixels. The substitution process will continue according to the ciphered message' s length. Random key concealed at the same 1st byte of the 4 cover image. The distortion being in the stego Image because of embedding a large amount of private messages using the offered method an undisclosed to human eye. Cover images that used are two standard RGB images Lena and Peppers and the message to hide was “I am Indian”, resulted PSNR between 70dB,75dB [9]

Noor K. hide information through creating the secret key and using the LFSR method, after that encrypt the secret message by using the AES method. The cipher text shared over the pixels of the cover image by using the technique of permutation. Then, in the cover image, hide the bits of the encrypted message in randomly picked pixels [10]. Ashwini and komal offered two methods for inserting the secret message inside the cover image, there are sequential and random encryption. The pixel for the embedding encrypted text acquired by applied XOR operation between the secret message and the key supplied by the user was sequentially picked using sequential encoding. The user provides two keys in random encoding there are one to locking the function on the receptor side and the other for performing the encryption. The pixels in this case are chosen at random to embed secret data, such as texts or images, using a generator of random numbers that implements the link list concept automatically. Cover image that used is 600*450 and the message to hide was “welcome to pote college”. The resulted PSNR of sequential encoding is 88.19dB and random encoding is 88.55dB [1] .

Elaf Ali Abbood, Shaymaa Abdulkadhm and Rusul Mohammed proposed a new method for hiding a secret message inside gray image by use a simple hash function, random technique, and secret key. The locations of secret message to the image dependent on secret message’s length. The secret message will be distributed over all the rows of cover image and in equal manner, and the last row was excepted, that have additional information was needed to hide. Fixed number of columns existent at each row, therefore this column exists needs for hiding secret message bits, that’s randomly chosen. The bits hide in column follows to a special schema. Cover images that used are three standard gray images Lena, Goldhill and Boat, the message to hide was 4900 bits, 5 14700 bits and 24500 bits, resulted PSNR between 52.9806dB, 60.0489dB [12].

Sabyasachi Pramanik1 and Ramkrishna Ghosh generated CAPTCHA codes that send in an encoded version. The CAPTCHA codes converted to its ASCII codes and those ASCII’s encrypted and then embedded into cover image that resulting the stego image and therefore attackers can’t extract the CAPTCHA code that resultant in a robust transmission of secret data through the internet and using the image steganography. Cover image that used is 24bit color image, the CAPTCHA code to hide was “B9@m#~2q.”, resulted PSNR is 42.56dB [13].

T.Kalaichelvi and P.Apuroop proposed new embedding technique that use a novel algorithm that is used for encrypting the CAPTCHA code. The length of CAPTCHA is between 8 and 16 characters. The randomized generated CAPTCHA code is converted to its ASCII codes, after that the ASCII codes is converted into its binary bit stream. Finally, the resulted binary is encrypted, and transmitted to the receptor. This technique used for identifying the intended receptor. Cover image that used is 24bit color image, the CAPTCHA code to hide was “^6h*?U>-.” [14]. Our method for hiding the secret text in the cover image was proposed in this paper, and that depend on the random number generation and developed method of LSB using an innovated encrypted algorithm.

3. The Proposed Method

In this paper proposed a new approach to hide a secret message in 24-bit color image using a secret key with random technique, innovative encrypt algorithm and LSB (Least Significant Bit). This paper main goal is to well hide the secret text to make it difficult for attacker or the third party to discover the text that will be hidden using the text-based CAPTCHA cover image and the design to improve security.

The steps of the approach were explained in following:
Step1 (convert each character of the secret text into its ASCII value): The secret message is a string that consist numbers, letters, and the special characters. Each one of characters converted to its ASCII value. For example: secret message is “code” converting it to ASCII value, the resulting values will be

c	o	d	e
99	11	100	101

Step 2 (Convert each ASCII value to the binary stream): Each ASCII value converts to 8 bits. For example: ASCII value is "118", when converting it to its binary, the resulting string will be "01110110".

Step 3 (prioritize the minimum number of occurrences of 0 or 1): If the minimum number presented is zero. The value of flag will be 0, else 1.

Step 4 (Create string of flag value, lesser occurrence and positions of lesser): Thus an ASCII value is not directly embedded into the cover image, rather flag value, number of occurrence of lesser 0’s or 1’s, positions where lesser number of 0’s or 1’s are taken place as string
For example: if the binary string "01110110". the flag value will be 0, the number of occurrence of 0 will be 3, positions of lesser will be 0,4,7 the resulting string will be “03047”

Step 5: (build a cipher text string): flag value stays the same and added to new string, lesser number would be converted to binary form and take just the right two bits add to new string of binary, positions of zero’s or one’s converted to binary form and take just the right three bits added to string of binary, new string of binary was built, this string is a cipher text
For example: if the string of flag and number of occurrence and positions is “03047”
0 =0
3 = 11
0 = 000 4 = 100 7=111
Resulting cipher text will be “0 11 000 100 111”

Step 6 (embedding cipher text to text-based CAPTCHA cover image using LSB embedding technique): embedding first binary bit of first encrypted character of secret text in fourth row position with random column position with specific range of cover image, use LSB embedding technique, complete other bits of encrypted character of secret text at the next positions of same row of the first binary bit position. Complete other encrypted characters at next rows while row=row+4 with random column locations

Step 7 (create and hide a secret key): create a secret key for each encrypted character by convert row position to binary bits string and generate a random number, will represent a part of a secret key and that will have converted to binary bits, that make a new binary stream of row and column that make a secret key, then start to store the binary bits of the first secret key from the pixel when row=0 at the same text-based CAPTCHA cover image using the LSB embedding technique. The other keys embedding at the next rows of the cover image and then sent image to the receptor.

When the stego image comes to the receptor, the receptor will extract the secret message by applying revers of the hiding steps. This steps of extract the secret message explained in the following:

Step 1: extract the secret key from cover image
Step 2: extract the row and column locations from a secret key
Step 3: extract the cipher text from the locations extracted from stego image using inverse LSB.
Step 4: from cipher text extract the string of flag value, number of lesser occurrence and positions of lesser occurrence.
Step 5: extract our binary string
Step 5: convert the binary string to its ASCII codes.
Step 6: convert each ASCII code to its character.
Step 7: secret text was extract.

4. Results

Our proposed approach used a good and safe scheme for hiding secret message in cover image. At this section shows the results after applying our proposed approach for hiding the secret text of different size and calculating the resulted images accuracy. All the above related work algorithms used two main tools to measure the accuracy of stego image, PSNR and MSE quality measurements. PSNR is the peak-signalto-noise-ratio, if the PSNR value increased the quality of image was increased. MSE is a mean-square-error, if the different between cover image and stego image small the quality of stego image was increased.

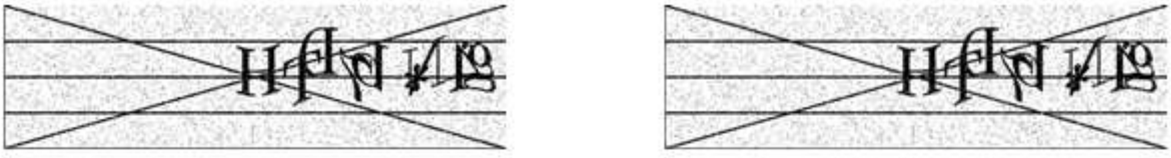
using MSE and PSNR that is described in Equation (1) and Equation (2), respectively

$$MSE = \frac{1}{MN}\sum_i \sum_j (\mathrm{y_{ij}} - \mathrm{x_{ij}})^2 \qquad (1)$$

$\mathrm{y_{ij}}$ indicated to the pixels of stego image and $\mathrm{x_{ij}}$ indicated to the values of cover image., and M, N indicated to the size of the cover image.

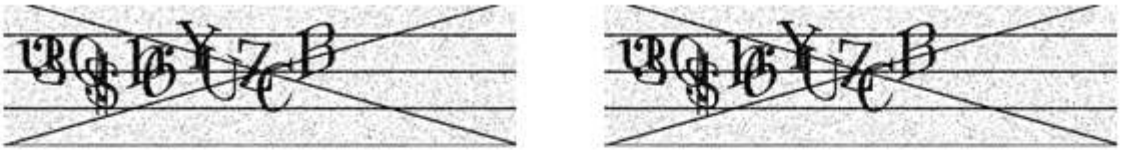
$$PSNR = 10log_{10}\left[\frac{255^2}{\frac{1}{MN}\sum_i \sum_j (\,yij - xij)2}\right] \qquad (2)$$

Figure 2, Figure 3 and Figure 4 show the effect of the proposed method on 194x698 text-based CAPTCHA cover image, 202x702 text-based CAPTCHA cover image and 202x699 text-based CAPTCHA cover image when hide a secret message with size 100, 90 and 80 bits, respectively.



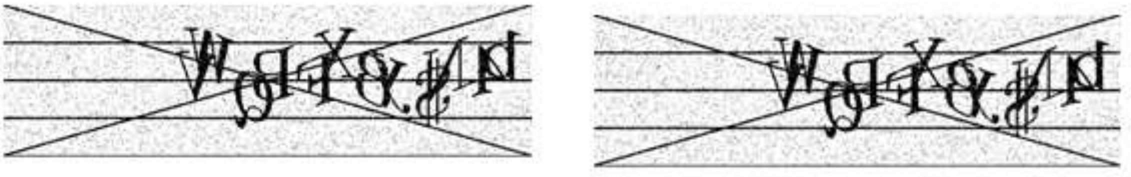
(a) The original image (b) The stego image

Figure 2. Hiding a secret text with size 100 bits in 194x698 text-based CAPTCHA image



(a) The original image (b) The stego image

Figure 3. Hiding a secret text with size 90 bits in 202x702 text-based CAPTCHA image



(a) The original image (b) The stego image

Figure 4. Hiding a secret text with size 80 bits in 202x699 text-based CAPTCHA image

Table 1: Shows the results of MSE and PSNR when applying the proposed approach on a different cover images and secret text with different size.

Cover image	Secret text 100 bits		Secret text 80 bits		Secret text1200 bits	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
194×698	0.00027	83.75234	0.00023	84.50274	0.00055	80.72718
202×702	0.00022	84.73407	0.00018	85.64903	0.00077	79,67982
202×699	0.00023	84.50284	0.00021	84.84182	0.00065	80.00167

330×572	0.00010	88,13080	0.00009	88,58838	0.00013	86.83581

5. Conclusion

The main benefit of developing approaches of hiding information for increasing the security of these road and for protecting information from being detection through the attackers. When we using our suggested approach, the message that hidden in the cover image that will not be directly hidden in the cover image and transmitted, instead, it will use other techniques for increasing the security of hiding and for strengthing the protection of the hidden information. As a result of using the innovative Encryption algorithm and the random selection of the position to hide information, a security obstacle was added to the proposed method of hiding data in front of attackers to keep confidential information from being tampered with, and this obstacle is one of the most important criteria for text steganography. also LSB technique is used to hides the secret text encrypted character’s bit in the lesser significant bits. And select the bit location in which we will for hiding 10 the random numbers was generated earlier. By using a text-based CAPTCHA cover image instead of a regular image, it was better because the image itself is distorted, and due to that reason any bot programs can’t distinguish any distortion in image and therefore can’t extract the message that hidden in the image.

Attackers may be able to get the hidden message inside the image successfully; they won’t get the secret message. Thy will only get the encoded form of the secret message. The algorithm was defined for the encryption and the decryption purposes only the intended receiver can successfully decrypt the encrypted message. Therefore, attackers will only get the encoded form of the secret message, and they cannot use information for their personal purposes.

By applying these steps, therefore increasing the security of the approach and give greater results in the terms of measuring the effect of the image after hiding compared to the original image.

References

1. Ashwini B. and Komal B., “Hybrid Approach for Embedding Text or Image in Cover Images”，*International Journal of Innovative Research in Science, Engineering and Technology*, vol. 5, no. 5, 2016.

2. Yang Ren-er and *et al*, "Image Steganography Combined with DES Encryption Pre-processing", *Sixth International Conference on Measuring Technology and Mechatronics Automation*, pp. 323-326, 2014.
3. Obaida Mohammad Awad Al-Hazaimeh, "Hiding Data in Images Using New Random Technique", *International Journal of Computer Science Issues*, vol. 9, 2012.
4. Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, 2001.
5. Rupali Bhardwaj and Vaishali Sharma," Image Steganography Based on Complemented Message and Inverted bit LSB Substitution", *6th International Conference on Advances in Computing & Communications*, 2016.
6. Ebrahim Alrashed and Suood Suood Alroomi, "Hungarian-Puzzled Text with Dynamic Quadratic Embedding Steganography", vol. 7, no. 2, 2017.
7. Reihane Saniei and Karim Faez, "The Security of Arithmetic Compression Based Text Steganography Method", *International Journal of Electrical and Computer Engineering,* vol. 3, no. 6, pp. 797-804, 2013.
8. Babita1 and *el al*, "An Approach to Improve Image Steganography using Random Key Generation Method", *International Journal of Information and Computation Technology*, vol. 3, no. 4, pp. 235-240, 2013.
9. Balvinder Singh and *el al*, "A Steganography Algorithm for Hiding Secret Message inside Image using Random Key", *International Journal of Engineering Research & Technology*, vol. 3, no. 12, 2014.
10. Noor Kareem Jumaa, "Hiding of Random Permutated Encrypted Text using LSB Steganography with Random Pixels Generator", *International Journal of Computer Applications*, vol. 113, no. 13, 2015.
11. Mojtaba B. and Karim F., "An Adaptive Steganography Scheme Based on Visual Quality and Embedding Capacity Improvement", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 4, no. 4, pp. 573-584, August 2014.
12. Elaf Ali Abbood, Rusul Mohammed Neamah, Shaymaa Abdulkadhm "Text in Image Hiding using Developed LSB and Random Method", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 4, pp. 2091-2097, August 2018.
13. Sabyasachi Pramanik and Ramkrishna Ghosh "A new encrypted method in image steganography" Indonesian Journal of Electrical Engineering and Computer Science, vol. 14, no. 3, pp. 1412~1419, June 2019.

14. T.Kalaichelvi and P.Apuroop “Image Steganography Method to Achieve Confidentiality Using CAPTCHA for Authentication” Fifth International Conference on Communication and Electronics Systems (ICCES) , 2020.