IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 8, August 2017

Information hiding by using Developed M8PAM Technique

Mustafa B. Mahmood[1], Ban N. Dhannoon[2]

Research Scholar, Department of Computer, College of Science, AL-Nahrain University, Baghdad, Iraq [1]

Professor, Department of Computer, College of Science, AL-Nahrain University, Baghdad, Iraq [2]

Abstract: As the result of increasing demand for the use of the Internet and applications that require storage and data transmission via the Internet, this data is being attacked by hackers. So appeared the need for data security. Researchers focused on devising different ways to keep this data from falling into the hands of intruders. There were encryption-decryption techniques and that are prone to doubt if it falls into the hands of hackers, so there was a need to use other techniques, one of these techniques is information hiding. The advantage of this technique it is not to keep intruders from knowing the hidden information, but it is to keep intruders from thinking that the information even exists. This paper is directed toward the task of steganography by using the developed method to hide every three bits from the secret message in one sample from the cover file and then adding a number to the product sample that represents the amount of central change, a proposed algorithm hides the secret message inside the popular images format which are frequently used in the Internet, this image format is known as a WebP format, also Known as the stickers for the chatting applications. Mod 8 Plus Average Method (M8PAM) is designed to hide the secret message inside a WebP image as a cover file. In this technique, the process of data hiding does not occur sequentially. So no distortion occurs in the carrier file which represents the cover file after the hiding process.

Keywords: Steganography, Mod 8 Plus Average Method (M8PAM), Central change.

I. INTRODUCTION

Information hiding is art and science of embedding the secret messages within other digital media such as image, video, Audio, text and protocols. Information hiding is called "Steganography", in Greek this mean "covered writing". The main goal of the Steganography to no doubt there are any important information in the Digital media when it falls in the hand of attackers. Steganography and cryptology are often confused with them because the two technologies serve the same purpose, is to ensure the security data. The difference between them is that steganography involves hiding information so it appears that no information is hidden at all. If a person sees the stego file that has hidden information, he should not be a doubt that the existence of any hidden information in it. Therefore the intruder will not try to extract the secret data[1] .The proposed method for information hiding requires fundamental elements for the completion of the works. These fundamental as shown in Figure (1) are:

1) The proposed algorithm (M8PAM) works in opposite directions, first: the process of data embedding. Second: the process of data extraction.
2) The secret data that needed to be protect from falling into the hands of the intruders.
3) The cover file, which will carry the secret data, it should be unaffected by the embedding process, as well as must keep its accuracy.
4) The optional key for increasing the security of the steganography system, this key maybe represented by symmetric key or maybe represented by the public-private key.
5) The stego file that represents the resulted of an embedding process.

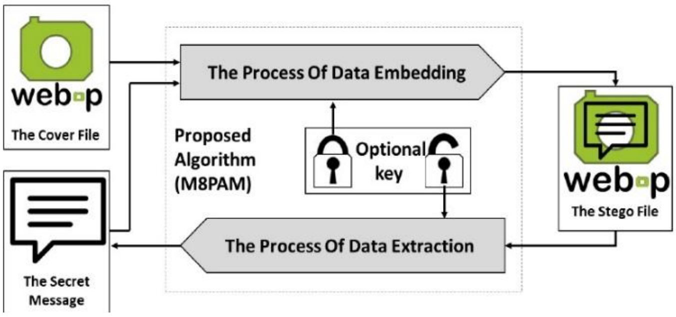

webp
The Cover File
The Process Of Data Embedding
Proposed Algorithm (M8PAM)
Optional key
webp
The Stego File
The Secret Message
The Process Of Data Extraction

Fig.1: The elements of the steganography system.

DOI10.17148/IJARCCE.2017.6802

There are basically three Steganography Types Figure (2) below shows the types of steganography techniques [2]: -

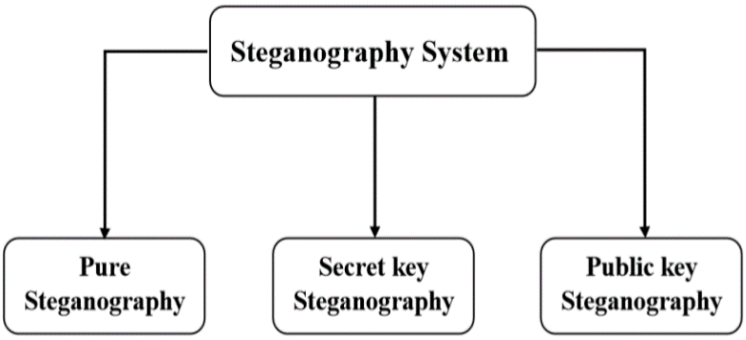


Fig.2: Steganography types

1) Pure-Steganography: A pure Steganography system that does not require the prior exchange of some secret information before sending the message.
2) Secret-key Steganography: A secret key Steganography It requires a prior exchange for information about hiding system that represents shared key on both sides.
3) Public-key Steganography: A public key Steganography It requires generating two keys for each user, the first key is the public key and used it for hiding information, and the other key is the private key and used it for extract hidden information.

II. LITERATURE SURVEY

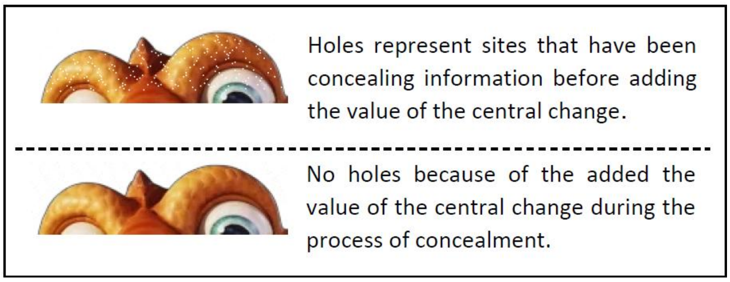
- Souvik B., Arko K., Gautam S.[3] proposed a novel audio based steganographic method for hiding information. The proposed approach works by selecting the embedding positions using some mathematical function and maps each four bit of the secret message in each of the selected positions in a specified manner. The proposed method can produce stego audio at various embedding rate with minimum or zero degradation. Besides Peak Signal to Noise Ratio (PSNR) value of the proposed method for various size of the secret message is very good.
- Shamim A., Kattamanchi H.[4] proposed a high capacity data embedding approach by the combination of Steganography and cryptography. In the process a message is first encrypted using transposition cipher method and then the encrypted message is embedded inside an image using least significant bit (LSB) insertion method. The Researcher will have two layers of protection. If a message is encrypted and hidden with a LSB steganographic method the embedding capacity increases. The method satisfies the requirements such as capacity, security and robustness which are intended for data hiding.
- Vipula M., Suresh K.[5] proposed algorithm using video steganography for enhancing data security, the secret message is already encrypted using Advanced Encryption Standard (AES) and Secure Hash Algorithm 1(SHA-1) it can be easily embedded into carrier video. Stego file is generated as a secret data is hided in the audio not in the image frames. Audio contains unused bits or free bits of information in which secret data can be very easily hided. Experimental results in more secure technique for data hiding. The proposed system is more effective for secret communication over the network channel.
- Debiprasad B., Kousik D., Jyotsna K., Paramartha D.[6] proposed a novel approach of building a secure data hiding technique in digital images. A secure LSB technique for image steganography has been proposed .The proposed algorithm provides added security to the base steganography technique. The proposed technique uses host image files in spatial domain to hide the presence of sensitive information . A 3-3-2 LSB insertion method has been used for image steganography. Experimental results show a substantial improvement in the PSNR and Image Fidelity (IF) value of the proposed technique over the base technique of 3-3-2 LSB insertion.
- Manjula G., Ajit D.[7] proposed method to embed a color secret image into a color cover image. A color image is considered as a cover media and secret data is embedded in this cover media as payload. The proposed technique takes eight bits of secret data at a time and put them in LSB of RGB (Red, Green and Blue) pixel value of the cover image in 2, 3,3 order respectively. Such that out of eight (08) bits of message five (05) bits are inserted in R and G pixel and remaining three (03) bits are inserted in B pixel. Experimental results show an improvement in the Mean squared error (MSE) and PSNR values of the proposed technique over the base technique of hash based 3-3-2 LSB insertion.
- Mohammed J., Atef A.[8] proposed a novel gray scale steganographic method for information security. It based on the idea of image segmentation to give an improved steganography method for embedding secret message bit in least significant bytes of random pixel in a random area within the grayscale cover image. Experimental results show that, the proposed method satisfied most of the security requirements (visual appearance, security, undetectability).

DOI10.17148/IJARCCE.2017.6802

III.THE PROPOSED TECHNIQUE

In this section, the researcher presents a new Technique for Information hiding. This technique named as Mod 8 Plus Average Method (M8PAM) along with using proposed algorithm to generate the consecutive indexes of the Cover media, which will be keeping the cover quality.

The secret message must be convert to stream of bits. The hiding process done by hide every three bits of the secret message in a selected index based on the remainder of the intensity value when divided by 8 and then adding with the value of central change that represent the value of amount of the difference between the value of the sites that are selected to embed the secret data before hiding process and the resulting value after the hiding process. Figure (3) below shows the difference between concealment process before adding the value of central change and after adding the value central change.



Holes represent sites that have been concealing information before adding the value of the central change.

No holes because of the added the value of the central change during the process of concealment.

Fig.3: The impact of adding the value of Central Change.

Extraction process starts by selecting site that carry the secret message. Then execute reverse process to get back the secret message.

Data embedding method: Algorithm (1) shows the implementation of the embedding process of the M8PAM.

Algorithm (1) implementation of the embedding process of the M8PAM.	
Goal: embedding the secret message inside the cover file. **Input:** The secret message as array of digits, the cover file as array of samples. **Output:** Stego File as array of samples.	
Steps:	**Example:**
- Step1: Read Array of the secret message as a digits.	**ArrayM={3,5,…..}**
- Step2: Read Array of the cover file as a samples.	**ArrayC={22,27,…..}**
- Step2: Set the variables to repeat step 3 and 5 until the end of the ArrayM And Initialization the Array to store the result .	**Loc = 0 , Index= 0** **ArraySte[ ]**

- Step3: For each digit in ArrayM And ArrayC Apply:
- Ocov = Cov= ArrayC[Loc]
- IF Cov **Negative, Then** Sign=-1 **Else** Sign=1
- Reminder = Cov **Mod** 8
- Cov = Cov – Reminder + ArrayM[Loc]
- Central Change[Ocover -Cov]++
- IF Sign = -1 **Then** Cov = Cov * -1
- Store the result
- Increment the index of location
- IF Loc **equal Size of** ArrayM **Then** go to step 4 **Else** repeat step 3
	
	Ocov=Cov=22
	Sign=1
	Reminder = 22%8 = 6
	Cov= 22 - 6 + 3 = 19
	CentralCh[22-19]++
	CentralCh[3]++
	Sign Not Equal -1
	ArraySte[Loc]= Cov
	Loc = Loc + 1

- Step4: Find the maximum value in Array of Central Change **Then** get it's index	Max=Max(CentralCh) Suppose: Max = 3
- Step5: For each digit in ArraySte Adding Central Change Value**:** **-ArraySte[Index] = ArraySte[Index]** + Max **-Increment the index of location** **-IF** Index **equal Size of** ArraySte **Then** go to step6 **Else** repeat step5	 **ArraySte[Index]= 19+3** **ArraySte[Index]= 22** **Index= Index+1**
- Step6: End	

The value 8 came to allow the possibility of hiding three bits from the secret message in every sample of the cover file, that's because the result of 2 power 3 equal 8, number 3 come to allow hide three bits but not more.

Data Extraction Method: Algorithm (2) the implementation of the extraction process of the M8PAM.

Algorithm (3.2) implementation of the extraction process.	
Goal: extracting the secret message from the cover file. **Input:** The Stego file as array of samples. **Output:** The secret data as array of the digits.	
Steps:	**Example:**
- Step1: Read Array of the Stego File as a digits.	**ArraySte={22,34,…..}**
- Step2: Set the variables to repeat step 3 until the end of the Size of the secret data, and initialization the Array to store the result .	**Loc = 0** **Index= 0** **ArrayM**

- Step3: For each digit in ArraySte Apply:
- IF ArraySte[Loc] **Negative**
Then ArraySte[Loc] = ArraySte[Loc] * -1
- Reminder = ArraySte[Loc] **Mod** 8
- **ArrayM[Loc]=** Reminder - Central Change
- Increment the index of location
- IF Loc **equal Size of** Message **Then** go to step 4
Else repeat step 3
	Sign=1
	Reminder = 22%8 = 6
	ArrayM[Loc]= 3 -3
	Loc = Loc + 1

- Step4: End	

IV. SYSTEM PERFORMANCE

Researcher in this section discusses the results of the proposed method based on the capacity of data hiding and the quality of stego cover, the quality of the cover should not be affected after the hiding operation. Standards adopted by the researcher that are hiding capacity, MSE and PSNR. This section presents three samples of different sizes Table (1) shows the length and maximum hiding capacity of each of the cover files.

TABLE I MAXIMUM HIDING CAPACITY OF EACH OF THE COVER FILES

Sticker 1	**Size of sticker**	**No. of Pixels**	**No. of R,G,B and Alpha.**	**No. of total locations**
	4530 Byte	30080 Byte	120320 Byte	21276 Byte
	Actual locations	**Size of message in byte**	**No. of maximum Char.**	
	14183 Byte	5318 Byte	2659 Char.	
Sticker 2	**Size of sticker**	**No. of Pixels**	**No. of R,G,B and Alpha.**	**No. of total locations**
	7242 Byte	32400 Byte	129600 Byte	24011 Byte
	Actual locations	**Size of message in byte**	**No. of maximum Char.**	
	16007 Byte	6002 Byte	3001 Char.	
Sticker 3	**Size of sticker**	**No. of Pixels**	**No. of R,G,B and Alpha.**	**No. of total locations**
	25948 Byte	262144 Byte	1048576 Byte	148075Byte
	Actual locations	**Size of message in byte**	**No. of maximum Char.**	
	98715 Byte	37018 Byte	18509 Char.	

Tables (2) and (3) shows the results of the comparison of the proposed algorithm with another algorithm called M16MA [3]. Where the results showed the preference of the proposed algorithm in terms of capacity and efficiency, the following measurements were used in the comparison process.

- **Mean Squared Error** between input signal and output signal.
- **Peak Signal-to-Noise Ratio** is the ratio between a signal's maximum power and the power of the signal's noise.

TABLE 2 MAXIMUM HIDING CAPACITY BY USING M8PAM AND M16MA.

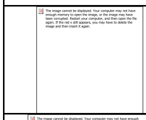
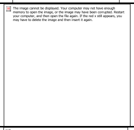
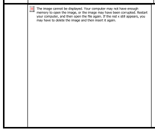
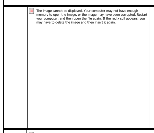
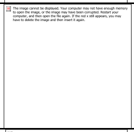
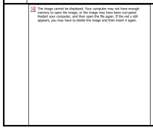
Sticker	Size of sticker	Algorithm	total locations	Actual locations	maximum capacity
 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.	6768 Byte	**M8PAM**	23484 Byte	15655 Byte	5870 Byte
		M16MA		2765 Byte	1382 Byte
 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.	12994 Byte	**M8PAM**	20742 Byte	13827 Byte	5185 Byte
		M16MA		2443 Byte	1221 Byte
 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.	31336 Byte	**M8PAM**	110081Byte	73387 Byte	27520 Byte
		M16MA		12954 Byte	6477 Byte

TABLE 3 THE DIFFERENCE BETWEEN THE RESULTS OF M8PAM AND M16MA THAT USED FOR COMPARISON

Sticker	Size of sticker	Algorithm	Size of Message	MSE	PSNR
 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.	6768 Byte	**M8PAM**	1237 Byte	0.0384 Byte	24.653 Byte
		M16MA		0.0385 Byte	24.640 Byte
 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.	12994 Byte	**M8PAM**	1013 Byte	0.0278 Byte	26.065 Byte
		M16MA		0.0318 Byte	25.489 Byte
 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.	31336 Byte	**M8PAM**	4059Byte	0.0147 Byte	28.841 Byte
		M16MA		0.0155 Byte	28.615 Byte

V. CONCLUSION

In this paper, a novel approach for information hiding is present, in this approach, every three bits of the secret message will be hide in one sample from the cover file then add the value to the produced sample that represents an amount of change Central, and are selected sites non-sequence from the cover and thereby ensure that no cover file confidential data deformation. The proposed method can produce stego file at various embedding rate with minimum or zero degradation. Experimental results show an improvement in the MSE and PSNR values of the proposed technique. The method satisfies the requirements such as capacity and quality of the stego file.

REFERENCES

[1] Abdelmgeid A., Tarek A., Al-Hussien S.,Shaimaa M.," New Image Steganography Method using Zero Order Hold Zooming", International Journal of Computer Applications, Volume 133 - No.09, January 2016.

[2] Jayaram P., Ranganatha H., Anupama H., “Information hiding using audio steganography-a survey”, International Journal of Multimedia and its Applications, Vol. 03-No. 03, August 2011.

[3] Souvik B., Arko K., Gautam S.,"A Novel Audio Steganography Technique by M16MA", International Journal of Computer Applications, Volume 30- No.8, September 2011.

[4] Shamim A., Kattamanchi H., "High Capacity data hiding using LSB Steganography and Encryption ", International Journal of Database Management Systems, Volume 04- No.6, December 2012.

[5] Vipula M., Suresh K., "Enhancing Data Security Using Video Steganography", International Journal of Emerging Technology and Advanced Engineering, Vol 03-Issue 04, April 2013.

[6] Debiprasad B., Kousik D., Jyotsna K., Paramartha D.,"A Novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain", International Journal of Security, Vol 03-No 01, February 2014.

[7] ManjulaG., AjitD., "A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain", International Journal of Security, Vol. 04-No.1, February 2015.

[8] Mohammed J., Atef A., "A Secure Robust Gray Scale Image Steganography Using Image Segmentation", Journal of Information Security, , Vol 07- No.3, April 2016.

DOI10.17148/IJARCCE.2017.6802