Steganography Using Reversible Dynamic Texture Creation

Dr. Ajit Kumar Rout, Dr. D K Bebarta

G.M.R. Institute of Technology, Rajam, Andhra Pradesh, India GVP College of Engineering for Women, Visakhapatnam. Corresponding Author; Dr. Ajit Kumar Rout

Abstract: In Communication system there is less security while transmitting the information. To avoid this, we have to use technique called Steganography. The art of hiding information in order to prevent detection of hidden messages is called Steganography. A novel approach for steganography is proposed using a reversible texture creation. In contrast to existing steganography algorithm, our algorithm conceals the source texture image and embeds secret messages through the process of texture creation. Here the embedded message may be hybrid version i.e. text or image. The process of texture creation converts a smaller texture image into a new texture image with similar local appearance and an arbitrary size. To conceal secret messages and the sourcetexture from a stego synthetic texture. The source image is divided into number of blocks and we have to compose new large image by randomly pastes all blocks of source texture image into some blocks of new image. Those locations are stored in index table. The remaining blocks are filled with secret message that may be text or image. For extracting message, we have to generate index table and we get back the source texture, and we have to perform texture creation, and extracting and authenticating the secret messages which is hidden in the stego synthetic texture.

Keywords: Steganography, synthetic, texture, authenticating, extracting.

Date of Submission: 20-01-2019 Date of acceptance: 05-03-2019

I. Introduction

In the last decade many advances have been made in the area of digital media, and much concern has arisen regarding steganography for digital media. Steganography is a singular method of information hiding techniques. It embeds messages into a host medium in order to conceal secret messages so as not to arouse suspicion by an eavesdropper. A typical steganographyapplication includes covert communications between two parties whose existence is unknown to a possible attacker and whose success depends on detecting the existence of this communication [1]. In general, the host medium used in steganography includes meaningful digital media such as digital image, text, audio, video, 3D model, etc. A large number of image steganography algorithms havebeen investigated with the increasing popularity and use of digital images.

Most image steganography algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image. This leads to two drawbacks. First, since the size of the cover image is fixed, the more secret messages which are embedded allow for more image

Distortion [2]. Consequently, a compromise must be reached between the embedding capacityand theimage quality which results in the limited capacityprovided in any specific cover image. Recall that image steganalysis is an approach used to detect secret messages hidden in the stego image [3]. A stego image contains some distortion, and regardless of how minute it is, this will interfere with the natural features of the cover image. This leads to the second drawback because it is still possible that an image steganalytic algorithm can defeat the image steganography and thus reveal that a hidden message is being conveyed in a stego image.

In this paper, we propose a novel approach for steganography is proposed using a reversible texture creation. A texture creation process resamples a small texture image which synthesizes a new texture image with similar local appearance and an arbitrarysize. We weave the texture creation process into steganography concealing secret messages as well as the source texture. In particular, in contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture creation. This allows us to extract the secret messages and the source texture from a stego synthetic texture. To the best of our knowledge, steganography taking advantage of the reversibility has ever been presented within the literature of texture creation.

Our approach offers three advantages. First, since the texture creation can synthesize an arbitrary size of texture images, the embedding capacity which our scheme offers is proportional

to the size of the stego texture image. Secondly, a steganalytic algorithm is not likely to defeat this steganography approach since the stego texture image is composed of a source texture rather than by modifying the existing image contents. Third, the reversible capability inherited from our scheme provides functionality to recover the source texture. Since the recovered source texture is exactly the same as the original source texture, it can be employed to proceed onto the second round of secret messages for steganography if needed. Experimental results have verified that our proposed algorithm can provide various numbers of embedding capacities, produce visually plausible texture images, and recover the source texture.

II. Literature Survey

Steganography is the art and science of hiding communication. A steganography system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. The term steganography literally means "covered writing". The objective of steganography is to communicate information in an undetectable manner such that when the messages are observed by unintended recipient there will not be enough evidence that the messages conceal additional secret data. Steganography is the objective of protecting secret information [4]. Typical steganography system consists of three objects: cover object (which hides the secret message), the secret message and the stego object (which is the cover object with message embedded inside it). Many different digital cover file formats can be used such as text, audio, image and video. However, given the proliferation of digital images, especially on the internet, and the large redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography [5]. There are numerous methods used to hide information inside of picture. In this Project we are used methods like Texture Synthesis and LSB technique.

Texture Synthesis is a process that resamples a small texture image which synthesizes a new large texture image with similar local appearance and an arbitrary size. We weave this texture synthesis process into steganography to conceal secret message. Firstly, a small source texture image is taken and is divided into number of blocks and we have to compose a new large image by randomly pasting all blocks of source image into some blocks of the new image, those locations are stored in the index table and thus obtain a secret key. The remaining blocks are filled with secret message that may be either a text or image. By using this Secret key, we can recover the source texture image at the destination side. After getting synthesized image we hide the secret message using LSB technique.

The least significant bit substitution is the important aspect used in this work. The change done on the rightmost bit of every pixel value is done by substituting a new value which is taken from the binary value of the data that is the text data in this work is replaced by the least significant bit or the rightmost bit in every pixel thus changing the value of the original data and embedding the required amount of data without making it visible [6]. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted.

The least significant bit (LSB) is the bit position in a binary integer giving the unit's value, that is, determining whether the number is even or odd [7]. The LSB is referred to the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is similar to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position [8]

It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used [9]. Normally, this is simply the exponent for the corresponding bit weight in base-2 (such as in $2^{31}.2^{0}$). The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits stay unchanged (000 to 000). Least significant bits are frequently employed in pseudorandom number generators, hash functions and checksums [10].

III. Proposed Algorithm

4.1 Algorithm:

4.1.1 Embedding Process:

The process of embedding secret message into the cover image in following manner. The following step by step is done at the **Sender's side**

- □ Step-1: Take source image and it is divided into patches
- \Box Step-2: Compose a new large image by placing these patches randomly in some places of new image.
- □ Step-3: Here we have to generate index table to record locations of source patches and secret key will be generated.
- □ Step-4: After getting Synthesized image we have to embed secret message that may be either text or image using LSB technique.
- □ Step-5: We obtain an stegosynthesized image which is sent to the receiver.

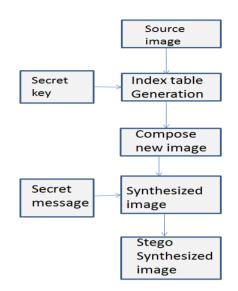


Fig-1: Embedding Process

4.1.2 Extracting Process:

The process of extracting the required secret message and recovering Original source image from the Stego Synthesized image is done in the following manner. The following step by step is done at the **receiver's side.**

Step-1: Take Stego Synthesized image and secret key

- □ Step-2: We have to generate index table using secret key to recover original source image
- \Box Step-3: We have to compose new image.
- □ Step-4: we have to extract secret message that may be either text or image using LSB technique.
- $\hfill\square$ Step-5: Thus we can obtain secret message.

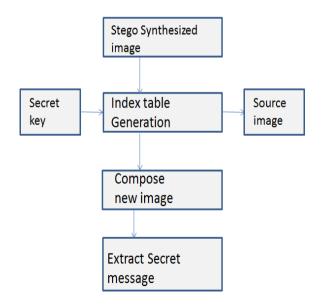


Fig-2: Extracting Process

IV. Results and Discussions

Hide Text:

The experimental results for different images used as the cover image and fixed data file are calculated by using the code mentioned above. The values in the below table represent the mean square error (MSE), peak signal to noise ratio (PSNR)[9] for the cover image after embedding the mentioned secret message in them respectively. The MSE and PSNR values are approximately same with different source images with fixed data file.

Source Image	Size of Data file	MSE	PSNR
Black weather (8.85kb)	1.31kb	0.0818	59.0015
Burlap (12.7kb)	1.31kb	0.0791	59.1498
Gxcejui (2.12kb)	1.31kb	0.0807	59.0619
Wrin (10.7 kb)	1.31kb	0.0847	58.8519

The experimental results for same image used as the source image and different data file are calculated by using the code mentioned above. The values in the below table represent the mean square error (MSE), peak signal to noise ratio(PSNR) for the source image after embedding the mentioned secretmessage in themrespectively. TheMSE is increasing with increase in the data file size. The PSNR is decreasing with increase in data file size. If MSE is low, it will be better. If MSE is low, then PSNR should be high.

Source Image	Size of Data file	MSE	PSNR
Black weather(8.85kb)	330 bytes	0.0194	65.2541
Black weather(8.85kb)	772 bytes	0.0460	61.5013
Black weather(8.85kb)	1.00kb	0.0612	60.2609
Black weather(8.85kb)	1.31kb	0.0818	59.0015

Hide Image:

The experimental results for different images used as the source image and same secret image are calculated by using the code mentioned above. The values in the below table represent the mean square error (MSE), peak signal to noise ratio (PSNR) for the source image after embedding the mentioned secret image in them respectively. The MSE and PSNR values are changing randomly with different source images with same secret image.

Source Image	Secret Image	MSE	PSNR
Black weather (8.85kb)	Lena (8.43kb)	26.2736	33.9356
Burlap (12.7 kb)	Lena (8.43kb)	30.2724	33.3203
Gxceju1 (2.12kb)	Lena (8.43kb)	27.7907	33.6918
Wrin (10.7 kb)	Lena (8.43kb)	27.3252	33.7652

The experimental results for same image used as the source image and different secret images are calculated by using the code mentioned above. The values in the below table represent the mean square error (MSE), peak signal to noise ratio (PSNR) for the source image after embedding the mentioned secret image in them respectively. The MSE and PSNR values are changing randomly with same source images with different secret image.

Source Image	Secret Image	MSE	PSNR
Black weather (8.85kb)	Lena (8.43kb)	26.2736	33.9356
Black weather (8.85kb)	Pot (53.5 kb)	44.8569	31.6129
Black weather (8.85kb)	Pepper (66.3 kb)	40.1811	32.0906
Black weather (8.85kb)	Jellybean (31.3 kb)	25.9788	33.9846

V. Comparison Between Existing System and Proposed System:

		Existing System		Proposed System	
Source Image	Size of the Data file	MSE	PSNR	MSE	PSNR
Black weather					
(8.85kb)	574bytes	0.03599	62.5683	0.03521	62.6632
Burlap					
(12.7kb)	780 bytes	0.04859	61.2645	0.04685	61.4225
GxeEJU1	1.00kb	0.0810	59.919	0.0807	59.0619
(2.12kb)					
Wrin	1.31 kb	0.0896	59.1510	0.0847	58.8519
(10.7kb)					

Steganography Using Reversible Dynamic Texture Creation

The above table shows the comparison from an existing system to a proposed system. As seen in the table the MSE and PSNR values of existing system to the proposed have slightly changes.

VI. Conclusion

In this paper we have presented a Steganography Using Reversible Texture Synthesis with the given input source images are texture images. We have to divide the source image into patches and place randomly in some places of new image. Those locations are stored in index table and a secret key will be generated. Then the synthesized image will be generated and the messageembeds into that. The Stego image and secret key will be sent to receiver side. With that, they will retrieve the secret image. In this model, the original source image will be recovered at the destination.

This model is robust and portable. This model has more hiding capacity compare to the existing system. In order to calculate distortion in the stego image, we use some parameters like MSE and PSNR. For better performance, MSE value should be low and PSNR value should be high. When compared to the existing system our proposed method shows better results in case of MSE and PSNR.

References:

- N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security Privacy, vol. 1, no. 3, pp. 32-[1]. 44.May/Jun. 2003.
- [2]. B.J.Mohd, S.Abed, B.Na'ami, "Hierarchical steganography using novel optimum quantization technique", Springer, SIViP 7:1029-1040 DOI 10.1007/s11760-012-0301-9, 15 March, 2012
- Steganography Using Reversible Texture Synthesis Kuo-Chen Wu and Wang Chung-Ming, Member, IEEE. JANUARY 2015. [3].
- [4]. M. F. Cohen, J. Shade, S. Hiller, and O. Deussen, "Wang tiles for image and texture generation," ACM Trans. Graph., vol. 22, no. 3, pp. 287-294,2003.
- K. Xu et al., "Feature-aligned shape texturing," ACM Trans. Graph., vol. 28, no. 5, 2009, Art. ID 108. [5].
- Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. [6]. 354-362, Mar. 2006.
- A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image [7].
- [8].
- N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26–34, 1998. T.Morkel, J.Eloff, M.Olivier, "An overview of image steganography", The Fifth Annual Information Security South Africa [9]. Conference (ISSAC), pp. 1–11, June/July 2005
- [10]. S.Gupta, A.Goyal, B.Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", I.J.Modern Education and Computer Science, vol. 6, pp. 27-34, June 2012 .
- Chung-Ming Wang a, Nan-I Wu a, "A high quality steganographic method with pixel-value differencing and modulus function", [11]. accepted 24 January 2007.
- A. A. Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," in Proc. 7th IEEE Int. Conf. Comput. Vis., Sep. [12]. 1999, pp. 1033-1038.