STEGANALYTIC ALGORITHM USING REVERSIBLE TEXTURE SYNTHESIS FOR EMBEDDING DATA


1ME, CSE, Student, Krisnasamy College of engineering and technology, Email:geethaparthy@gmail.com
2Assistant Professor, ,Krisnasamy College of engineering and technology, Email:priyamuthukumarang@gmail.com
3ME, CSE, Student, Krisnasamy College of engineering and technology, Email:abiramisanju92@gmail.com

Abstract: - Stenography is to hide the secret information within the cover image. The word stegno means “covered “and graph means “writing”, therefore it used to write the secret data on cover image. The steganalytic Algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. We weave the texture synthesis process into stenography to conceal secret message that allows extracting secret images and source texture synthesis from the stego synthetic structure. In video texture synthesis is the process of providing continuous and infinitely varying stream of frames, which. Embedding is a process to embed the secret images into cover images. Images data hiding is a technique for increasing the embedding efficiently .In the existing method, secret information is hidden in cover image. In this project, steganalytic algorithm using reversible texture synthesis method is used to resample the smaller texture image and which synthesis a new texture image with a similar local appearance and arbitrary size. In line based cubism like image segmentation is used to embed the data, but we propose reversible texture synthesis for embedding the data which improves the data embedding without any distortion.

Key words: Texture synthesis, secret data embedding by using reversible texture synthesis. Stego image, cover image, optimal value transfer.

1. Introduction

In this method the message is embed into a host medium and which conceals the secret message efficiently. The steganalytic algorithm used to cause the cover communication between the patches. And used to extract the source texture, secret message from original image .This image looks similar to the original image. In line based cubism like image segmentation technique is used to embed the data but it only stores the limited data. we propose a
stenography using reversible texture synthesis technique. Reversible texture synthesis is the process of embedding the secret message on the cover image. The image is said to be stego image after embedding the data on cover image. Reversible texture synthesis process of re-samples a smaller textures of original image and produce the output which is similar to the local appearance of source image. Our approach provides an advantage in arbitrary size of texture synthesis, which improves embedding efficiency. Secondly, it provides the source texture without any modification. Reversible data hiding to provide the capacity of better embedding process. Finally steg analytic algorithm is used to extract the source texture. Stenography technique used in various applications such as military application, cryptography, and video texture synthesis. In military application the secret message transformation done by using this stenography technique. Cryptography embeds the encrypted data.

2. Existing system

Texture synthesis is the process performs a major role in a graphics and visioning video texture synthesis process it takes the video stream as an input and produces the output video stream by texture synthesis only on particular temporal domain. Two types of algorithm used one is pixel based algorithm another one is patch based algorithm. In pixel based algorithm most similar pixel is produced as an output and rest of the pixels are retrieved by data detection mechanism. In patch based algorithm first choose the source texture and then choose the candidate texture. After choosing the candidate texture identify the boundary gap between source texture and candidate texture by using dynamic programming. In this stenography technique the size of the stego image is compared with original file. The image after embedding the secret message is called “stego image”. From this stego image the source texture had been retrieved.
3. Proposed system:

It provides a secure data embedding efficiency because the size of the cover image is vary depends upon the secret message. this will make to store large amount of information. the stego analytic algorithm is used to extract the secret message from source texture. The distortion of image is very low in our opposed system. Reducing distortion is the crucial issue in existing method this will overcome by our system. Identification of LSB location is not necessary for embedding data the data embedding performed based on RGB range of an image.

- Loading message and image
- Conversion process
- Better value transformation
- Verification and validation
- Extracting secret message

These are all the various methodology to embed the data to cover image. message embedding procedure reduces the deduction of message. Our system improves the solution space and also reduces the computational complexity.

4. Architecture:
The message and image is loaded by using GUI format. Then for the message and image binary conversion will be performed. Uniform embedding design is used to embed the message into cover image. Binary converted value of ASCII code and RGB value to be embed after the conversion. Then the secret key used to append the value of bits. Finally secret message will extract by receiver.

4.1 Loading message and Image:

User can enter into login page by an authenticated username and password. The username and password should be valid then only we can enter into login page. Then, the choosing of an image path process should be performed. The selection of image path is user specified. It depends upon the user who selects their image from any location. Then the selection of image did by the user for embedding purpose. the selected image then placed on a square like format. Then enter the secret message which we desire to embed on that cover image. Then the secret message and image had been embedded by using GUI.

4.2 Conversion process

Binary conversion carried out for both image and secret data. First for the image, The RGB range of an image has been taken and then corresponding binary value will be obtain. Next the embedded text has been taken and the word taken as individual character it will convert firstly as related ASCII code. Secondly for that ASCII code will convert as binary 8 bit code. each and every time the 8 bit will get add. For the first character length of the word is 8 bit .For the next character the length is 16 bit like wise it goes on. The larger the cover message is (in data content terms—number of bits) relative to the hidden message, the easier it is to hide. Image Conversion of red, green and the blue as well we can get one letter of ASCII text for every three pixels.

For example: a 24-bit bitmap will have 8 bits representing each of the three color values (red, green, and blue) at each pixel. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. If we consider just the blue there will be 28 different values of blue.

4.3 Better value transformation:

The appending of bits done at the end of the image’s RGB converted bit .the indicator performs a major role in a appending process. If the ending off bits like 00 no bit should be append .if the ending of bit is either 01 or 10 means 3 bits will append or else if 11 will be the ending of RGB bit then add 4 bits. All these process should be done at the end of the image’s RGB binary converted bits. The Optimal transfer matrix for illustrating the modification of cover values in reversible data hiding. Then, an iterative procedure is proposed to calculate the optimal value transfer matrix, which will be used to realize reversible data hiding with good performance. Matrix Embedding by Matrix Extending method and produces a stego object with least distortion under the tree based parity check model.

4.4 Embedding process:

The original matrix embedding, when the number of random columns (K) increases, the solution space of is exponentially expanded, and thus we have more chances to find a solution with smaller Hamming weight. That is why the embedding efficiency can be improved when increases, but the computational complexity of searching for this solution exponentially grows. In this section, we propose a novel method, by which we can also exponentially expand the solution space, but only cost linearly increasing time to search the solution space. The key idea of the proposed method is to append some referential columns to the matrix.

The MEME can produce a stego-tree. In our proposed we solved Two critical issues for a steganographic method i

1) Reducing distortion on cover objects
2) Better efficiency for embedding and extraction. These two critical issues are resolved by Matrix Embedding by Matrix Extending.

4.5 Verification and validation:

Color Filtering:
The Stego image gives information about the gradient intensity of red, green, and blue (RGB) wavelength regions in the digital image. Sheinberg illumination to highlight different textures on the is a very accurate color filter used to selectively pass light of a small range of colors while reflecting other colors.

Weight Estimation:
Estimation of the infarction by using distortion weighted imaging (DWI) and quantitative measures of distortion. It's a procedure to estimate the distortion tensor from a sequence of distortion-images. To check whether the image has been created by adding different types od distortion of original mage.

4.6 Extraction of secret message:
The embedding and extraction, a location finding method determines a sequence of locations that point to elements in the cover object. The embedding algorithm modifies the elements in these locations to hide message and the Reversible steganalytic algorithm can recover the message by inspecting the same sequence of locations. The steganalytic algorithm using reversible texture synthesis process is used to extract the source texture from original image .this also extracts the secret message.

Application

- Stenography can be used anytime you want to hide the data.
- Terrorists can also use steganography to keep their communications secret and to coordinate attacks.
- All of this sounds fairly nefarious, and in fact the obvious uses of steganographic are for things like espionage.
- But there are a number of peaceful applications.
- The simplest and oldest are used in map making, where cartographers sometimes add a tiny fictional street to their maps, allowing them to prosecute copycats.
- A similar trick is to add fictional names to mailing lists as a check against unauthorized resellers.

FUTURE ENHANCEMENT

The Matrix Embedding by Matrix Extending, we effectively construct the stego object with least distortion under the tree structure model. We also show that our method yields a binary linear stego-code. In comparison with the Matrix method, our method significantly reduces the number of modifications on average. To combine other steganographic approaches to increase the embedding capacities.
Conclusion

The optimal transfer mechanism proposed in this work is independent from the generation of available cover values. Our algorithm can produce visually plausible stego image even if the secret messages consisting of bit “0” or “1” have an uneven appearance of probabilities. The presented algorithm is secure and robust against an RS steganalytic attack. In other words, the optimal transfer mechanism gives a new rule of value modification and can be used on various cover values. If a smarter prediction method is exploited to make the estimation errors closer to zero, a better performance can be achieved, but the computation complexity due to the prediction will be higher.

REFERENCES


[5] Ioan-Catalin Dragoi, Member, , Dinu Coltuc, Senior Member, “Local-Prediction-Based Difference Expansion Reversible Watermarking” IEEE Transaction on Information forensics vol. 23, no. 4, April 2014

Author’s profile

P. GEETHA is presently pursuing her M.E degree in computer science and Engineering from Krishnasamy college of engineering and Technology, Cuddalore, TamilNadu, India. She has received her B.E degree in C.S.E from VRS College of Engineering, Arasur, villupuram,, TamilNadu, India in 2013. Her research interests are in the areas of image processing and web designing.

K. PRIYA received BE CSE degree from University of Madras and M.tech CSE degree from SRM University, Chennai. She is working as Assistant Professor in department of Computer Science at Krishnasamy College of Engineering and Technology, Cuddalore, TamilNadu. She is having 12 years of teaching experience. Her area of interest is image processing. She has guided the projects in image process, network security, cloud computing.

N. ABIRAMI is presently pursuing her M.E degree in computer science and Engineering from Krishnasamy college of engineering and Technology, Cuddalore, TamilNadu, India. She has received her B.E degree in C.S.E from Dhanalakshmi College of Engineering, Chennai, TamilNadu, India in 2013. Her research interests are in the areas of image Segmentation and image processing