International Journal of Computer Science and Engineering Communications,
Vol.4, Issue.1, Page.1281-1283, (2016)
www.scientistlink.com

A Comparative Study on Pattern Based Image Steganography

Sumathy Kingslin[1],R. Anusuya[2]
[1]Research Supervisor, [2]Research Scholar,
Department of Computer Science,
Quaid E Millath Government College for Women, Chennai, India
sumathy.research@gmail.com[2], anu7690@hotmail.com[2]

Abstract – *The speedy growth of the Internet and digitized contented made text/image delivery simpler. The capability to protect and secure information is dynamic to the growth of electronic trade and to the growth of the Internet itself. A safe data transmission over computer networks can be realized concluded steganography and cryptography. Steganography is a technique used to transmit a secret message from a source to a receiver in a way such that a probable intruder does not suspicious the being on the message. In steganography different-different carrier files can be used, but the most popular is digital images because they are used a proportion now a day on the internet. Steganography helps in the communication of secured data in numerous carries like images, videos and audio. In image steganography the information is hidden entirely in images. A comparative study on pattern based image steganography, one of the drawbacks of most of the current steganography methods is that it changes the bits used for storing color information. A comparative with different three methods of steganography, pixel pattern, 3D pattern, Dynamic pattern. [1,10]In this Paper, means to give an overview of image steganography, its uses and techniques. It also endeavors to classify the requirements of a good steganography algorithm using pattern based and briefly reflects on which steganography techniques are more suitable for this pattern based steganography*.

Keywords: *Steganography, DPIS, pixel, 3D steganography, Data Protection, LSB, Cover Image*

1. Introduction

The communication technologies from place to place has grown at a great speed in recent times. For swapping of data/ information on these days the whole world is depending of high speed, computer networks like the internet which is quite insecure and information can get wide-open. Massive amount of personal data is often collected, used and transferred to third party administrations for a variety of details. Hence, data security is becoming a serious problem in data communication via the Internet or any other media. We can use Steganography, or Cryptography to keep sensitive data. Steganography is regularly considered better than cryptography because the proposed secret message does not attract attention to itself for analysis.

2. Dynamic Pattern Image Steganography

Steganography is the art of hiding top-secret evidence in mass media such as image, audio and video. The purpose of steganography is to obscure the existence of the top-secret information in any given medium. This work aims at consolidating the safe keeping in the steganography algorithm by producing dynamic pattern in the selection of pointer arrangement. In addition to this dynamicity is also encompassed in number of bits embedded in data channel. This method has been executed and the consequences have been compared and calculated with current similar methods. In this paper, we propose a Dynamic Pattern based Image Steganography (DPIS) technique for RGB based image steganography. [2,3,5] DPIS technique makes sure lowest capacity for storing top-secret message than existing techniques and it also makes sure that stations containing comparatively lower color standards can store more bits of data. New outcomes show that our technique achieves much better than the existing techniques.

In this paper, dynamic pattern based image steganography technique has been brought together. This technique addresses key significant subjects like dynamicity in data embedding and indicator sequence and thus making it problematic to hack by steganalyst. Additionally, it also notices whether the stage image has been altered by an intruder throughout transmission. DPIS technique outcomes in very high capacity with low visual distortions and all this have been proved by new results. DPIS technique has also been compared with important features of other steganography algorithms.

Features	RGB Intensity based variable bits	Pixel Indicator	DPIS Technique
Indicator Sequence	Vary in length of 3	Static	Variants with different length
Brute force attack	Breakable	Breakable	Not breakable
Number of bits embedded in data channel	Static and depends on partition schema	Static	Dynamic and its decided at run time
Sequential data embedding in all pixels	Yes	No	No
Tampered stego image detection at decryption part	Not possible	Not possible	Possible

3. Pixel Pattern Based Image steganography

One of the weaknesses of the existing steganography techniques is that it changes the bits used for storing color information. There are also various prevailing methods like Dynamic RGB Intensity Based Steganography Scheme, Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm, etc. that can be used to find out the steganography method used and break it[6]. And it adds noise to the image is also one of the drawbacks which will make the image as dull and grainy, making it suspicious of a person about the existence of a hidden message within the image. To overcome these weaknesses we have come-up with a pixel pattern based steganography, which elaborate hiding the message within an image by using the existing RGB values at any time possible at pixel level or with minimum changes. Laterally with the image a key will also be used to decrypt the message stored at pixel levels. For further protection, together the message stored as well as the key file will be in encrypted format which can have same or different keys or decryption.

It always deals with an embedding algorithm for secured encrypted messages in nonadjacent, and random pixel locations in edges and smooth areas of images. The randomization will growth the security of the system and it also increases the capability. The steganography techniques are improver values of red, green, and blue. This pixel pattern based steganography algorithm is not only hidden the message behind the image, and also protect more secure than others. In this purpose, encryption technique is used with a user-defined key. In this method, the message has been protected in the image in the form of the image, which is used for the image generation method. In Pixel indicator, a high capacity technique for RGB Image based steganography give the thoughts from the random pixel manipulation methods and they stegokey ones techniques are combined, which uses the least two significant bits of one of the channels to indicate survival of data in the other two channels (G, B)

1. Using DES or RSA or any other encryption algorithm to encrypt the steganographic program.
2. Find out the pixel values of all the pixels within the image in steganographic program.
3. The unique RGB modbit method is used in steganographic program, to find out each and every letter of the message can be represented in the image and records the position of a field in the image metadata itself.
4. Select an image
5. Provide the image to stegano application
6. Gets encryption key.
7. Writes the encrypted image

Data extraction process

1. Inputs stegano image
2. Gets encryption key
3. Decrypts text and shows it

This technique is more secured, this research was pointed towards the growth of a new and better data hiding technique based on RGB based steganography without changing the image. Some of the possible presentation areas include hands on small

secret messages, using an image as a password token by encrypting and hiding password using this technique, simply adding a hidden signature to an image etc.

4. Pattern Based 3D image steganography

This method proposes a new high capacity steganographic scheme using 3D geometric model, the novel algorithm re-triangulates a part of a triangle mesh and embeds the secret information into a newly added position of triangle meshes. In this proposed method is experimental results show that algorithm is more secure, with high capacity and a low distortion rate. This algorithm is attack compared to uniform transformation such as cropping, rotation and scaling. The act of the method is compared with other existing 3D steganography algorithms. Now a days three-dimensional 3D geometric models are fetching an important portion of the multimedia at ease. There are valued products of knowledgeable activities in the computer graphics field. In this 3D method, a new technique for embedding information into 3D geometric models by building triangle meshes. The proposed algorithm re-triangulates a portion of a triangle mesh and embeds the secret information into the locations of the anew added vertices. Up to 9 bits data can be invisibly inserted into a vertex of the triangle without effecting any changes to the geometrical configuration and visibility of the original 3D image model the inserted helped information resists many of the geometrical attacks.

5. Conclusion:

Analyzing three techniques of Dynamic, Pixel and 3D pattern based image steganography are message is embedded into cover image and data should be more secure with decrypt key. Pixel pattern based image steganography are images are divided into pixel and using RGB to send the data without noisy. 3D pattern based image steganography are very secure, but the stegoimage should be in distortion. Dynamic pattern based image is more secured, integrity, confidentiality of the data. The secret message is embedded using DPIS algorithm is more secure and better result could be produced in this paper.

Reference:

[1] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioum, Abdulrahman Shaheen and Aleem Alvi, “Pixel Indicator High Capacity Technique For RGB Image Based Steganography, WoSPA 2008 – 5th IEEE International
Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah,U.A.E 18- 20 March 2008

[2] Anderson RJ, and Petitcolas FAP, “On Limits Of Steganography”, IEEE Journals of selected areas in communications, May 1998

[3] Andreas Westfeld , Andreas Pfitzmann, Attacks On Steganographic Systems, Proceedings of the Third International Workshop on Information Hiding, p.61-76, September 29-October 01, 1999

[4] Bailey K, Curran K. “An Evaluation of Image Based Steganography Methods” Multimedia Tools & Applications, Vol.30.No.1.pages 55-88 July 2006

[5] Krenn R, “Steganography and Steganalysis”,http://www.krenn.nl/univ/cry/steg/article.pdf

[6] Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub, "RGB Intensity
Based Variable-Bits Image Steganography," apscc, pp.1322-1327, 2008 IEEE asia-Pacific Services Computing Conference, 2008