IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VII (Sep – Oct. 2014), PP 130-135
www.iosrjournals.org

Using Concept of Steganography and Visual Cryptography for Secured Data hiding

Mr. Deepak S. Bhiogade, Prof. Milind Tote
Dept. of Computer Technology Nuva College of Engineering & Technology, Nagpur, India
Dept. of Computer Technology Gurunanak Institute of Engineering & Technology,Nagpur, India

Abstract: *The most advanced and updated Shamir Encryption algorithm is efficient enough to prevent and stop unauthorized and illegal access to the secured encoded data. It is best to solution to ensure reliability and security of the data with the help of Steganography and Visual Cryptography. On the ground of the failure of the previous extensive research by expert to ensure security of the data.*
Index Terms: *Data hiding, Efficient, Integrity, High performance, Reliable, Secured.*

I. INTRODUCTION

Steganography is the art, Science, or practice in which messages, images, or files are hidden inside other messages, images or files. The person sending the hidden data and the person meant to receive the data are the only once who know about it, but to everyone else, the object containing the hidden data just seem likes an everyday normal object. When it comes to the data transformation algorithms Steganography and Visual Cryptography take advantages of different methodology in order to protect their respective payload. In steganography, only the sender and receiver aware of the hidden data and typically if the loaded file thing that comes to their mind is the question of what is the encrypted and how they can decrypt the hidden message .

Steganography is concern with sending a secret message while hiding its existence. The word steganography is derived from the Greek words Steganos, meaning "Covered", and Graphein meaning "To Write".

Cryptography is not concerned with hiding the existing of message, but rather its meaning by a process called Encryption. The word Cryptography derived from the Greek word Kryptos, meaning "Hidden".

Seganography embed the secret message in a harmless looking cover, such as digital image file. The need for steganography is obvious but what is less obvious is the need for more research in the field. Simple techniques are easily detectable and there is a whole field of defeating steganographic technique called steganalysis, advances in steganalysis which makes it constantly evolving field. Since most steganography system use digital image as cover, the whole field has borrowed methods and ideas from the closely related field of watermarking and finger printing which also manipulate digital audio and video, for the purpose of copyright. Even though, in principle, many aspect of image can be manipulated, in reality most stego system aim for the preservation of visual integrity of the image. Early Stego system goals were to make changes not detectable by the human eyes. This feature is not enough because statistical method can detect the changes in image even if it is not visible. Image compression also plays a role in steganography because it was found at on many occasion the result depend on the compression scheme used. Steganography struggle to find more efficient method to embed a secret message in cover object, only to be defeated by techniques derived by steganalysts.

II. LITERATURE REVIEW

Steganography and visual cryptography had so far been dealt with as two separate entities as far as possibilities of use. A few algorithm touches on the concept of using Steganography and visual cryptography together, such as the JVW method mentioned above. JVW mentions the use of watermarking, embedding another image inside an image, and then using it secrete image. The secrete image would get split into shares which would need to be overlaid to reveal that secrete image. The use of Steganography alongside visual cryptography was a strong concept and adds a lot of challenges to detecting such hidden and encrypted data. For example, imagine an algorithm which uses one of the strong algorithms of Steganography to hide data inside an image, and they uses that image as a secrete image with a strong visual cryptography method. Basically we would then have a secrete image with hidden data which would be split up into shares. These shares can also be innocent images, not necessarily noise images. Then when these shares were reassembled or decoded to reconstruct in original image we would then have a revealed image which still contains the hidden data. So the receiver would be able to extract the hidden data from the revealed image. This algorithm cannot exist without having a perfect reconstruction property in the visual cryptography method. The reason for that was that if our reconstruction process or even the encryption process alters the image data, then it would consequently alter our hidden data which would make it impossible to extract the hidden data from the revealed image.