TRANSMISSION OF ENCRYPTED IMAGE OVER A NETWORK WITH HIGH SECURITY

Mohammad Sajid Qamruddin Khizrai¹ and Professor S.T Bodkhe²

¹PG Scholar, Priyadarshini Institute of Engineering & Technology, Department of Computer Science and Engg., Nagpur, INDIA
²Professor, Priyadarshini Institute of Engineering & Technology Department of Computer Science and Engg., Nagpur, INDIA

ABSTRACT

The security of and information is being used from an ancient age. In an ancient age the information was also hiding using different methods called steganography. It is the process of securing information behind any one or many of the other images. Now a day’s steganography is also using for image security, but most widely used method is encryption and decryption. Image Encryption is a process of hiding image from unauthorized access with the help of secret key that key can be private or public. It is used in many areas where the security risk is very high.

The encryption and decryption mechanisms will improve the security. Information security is a very important issue in this world, when the information is transfer from one geographically location to another geographically location through network there is chance of steal of information through network.

Generally information is encrypted and decryption using one encryption key and one decryption key for information such as image. In our proposed work an image is encrypted in various parts using different keys, for each part of the image. Now a day’s parameters (like Bandwidth, Storage, and time etc.) are not the problem when security is matter.

Keywords: Image Encryption with High Security.

1. INTRODUCTION

As the world changes rapidly technology is also changing rapidly. In advancement of network technology, large amount of multimedia information is transmitted over the Internet conveniently. Various confidential data such as Banking and other secured data, space images taken using satellite and commercial identifications are transmitted over the Internet. While using secret information we need more secure information hiding techniques.
In our proposed method we are securing information sixteen times instead of one in a single information transmission.

2. RELATED WORKS

The concept of the mosaic images was created perfectly and it has been widely used. Four types of mosaic images namely crystallization mosaic, ancient mosaic, photo mosaic and puzzle image mosaic are proposed in [2]. In the first two types, the source image is split into tile image and then it is reconstructed by painting the tiles and they are named as tile images. The next two types include obtaining target image and with the help of database, cover image has been obtained. They may be called as multi-picture mosaics. The previously mentioned mosaic image namely crystallization mosaic uses voronoi diagram which was proposed in [3]. The main concept of voronoi diagram includes by using different sites. The blocks are placed in the sites randomly. Based on the original image, the blocks are being filled by the colors.

The emerging Visual Cryptography (VC) techniques used in the secure transfer of the thousands of images collected by the satellite which are stored in image library and sent to Google for use on Google Earth and Google maps. The related work is based on the recovering of secret image using a binary logo which is used to represent the ownership of the host image which generates shadows by visual cryptography algorithms [4]. An error correction coding scheme is also need to create the appropriate shadow. The logo extracted from the half-toned host image identifies the cheating types. Furthermore, the logo recovers the reconstructed image when shadow is being cheated using an image self verification scheme based on the Rehash technique which rehash the halftone logo for effective self verification of the reconstructed secret image without the need for the trusted third party (TTP).

One of the best known techniques to protect data such as image is Visual cryptography [4]. The visual cryptography scheme as a simple and secure way to allow the secret sharing of images without any cryptographic computations [5] VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. The basic scheme is referred to as the -out-of- VCS which is denoted as VCS. Given an original binary image, it is encrypted in images, such that where a Boolean operation is an image which appears as white noise, and is the number of noisy images [6]. It is difficult to decipher the secret image using individual’s. The encryption is undertaken in such a way that one or more out of the generated images are necessary for reconstructing the original image. In the case of (2, 2) VCS, each pixel in the original image is encrypted into two sub pixels called shares. The concept of visual cryptography using visual information pixel (VIP) in [4] synchronization and in diffusion error to attain a cryptography encryption method for color visual, that produces meaningful color shares with high quality visualization in [7] and [9]. Synchronization in VIP retains the pixels positions that carrying visual information of original images throughout the color channels and diffusion error generates shares pleasant to human eyes. In [4] color VC encryption method which leads to meaningful shares and is free of the previously mentioned limitations.

The method (idea) is simple and efficient. It relies on two fundamental principles (rules) used in the generation of shares, namely, diffusion error and Synchronization in VIP. Diffusion error is a simple but efficient algorithm for image halftone generation. The error in quantization at each pixel is filtered and (regenerate for next) fed to future inputs.

3. PROPOSED RESEARCH METHODOLOGY

In our proposed work we will read a image (A) by using some command OR algorithm we will divide the image in to I*I parts i.e. (2*2, 4*4) parts. Each part of the image will be treated as a
single image we can say that IMG1, IMG2, IMG3 … IMGn. The output of the above i.e. IMG1, IMG2, IMG3 … IMGn, and each parts of the image is treated as a single image. And using different encryption algorithm, we will encrypt each images, we can say that encrypted images (Encrypted images= EIMG1, EIMG2, EIMG3 …EIMGn). After that we have two options

1) We can transfer all sub encrypted images EIMG1, EIMG2, EIMG3 … EIMGn at receiver side.
OR
2) We can combines (Merges) each all encrypted images EIMG1, EIMG2, EIMG3 … EIMGn. And make a single encrypted image A1, for transfer.

REFERENCES

[6] Resolution Variant Visual Cryptography for Street View of Google Maps Jonathan WeirWeiQi YanQueen’s University Belfast Belfast, BT 7 1NN

AUTHOR’S DETAIL

Mohammad Sajid Qamruddin Khizrai received the B.E (Computer Technology) 2002 and Pursuing M.Tech degrees under the guidance of Prof. S.T Bodkhe in Computer Science and Engineering from Priyadarshini Institute of Engineering Technology in 2013 and 2014. During 2006, he worked in “Doha Asian Games 2006” as Wi-Fi Technician in Doha Qatar. In 2007-2008 he has also worked as Computer Lecturer and Network Technician in King Saud University in Kingdom of Saudi Arabia.