IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
NCRTET-17
National Conference on Recent Trends in Engineering & Technology
Government Polytechnic College Kasaragod, Kerala
Vol. 4, Special Issue 1

Image Transmission Techniques

Neena M K

Lecturer, Computer Engineering, Women's Polytechnic College, Thrissur, Kerala, India

Abstract: Applications of digital image processing become more common, especially as the transfer of images from one entity to another using the internet as the medium of transfer is increasing. Digital image transmission technology has found advanced applications in various areas where security is of paramount importance. Examples of such applications include medical databases and confidentiality of patient records and information's, military databases and prevention of leaking of classified materials, business databases and protection of enterprise-wide records; online document storage systems, etc.This paper reviews Digital image encryption and mosaic image transmission are two approaches to secure image transmission.

Keywords–database, encryption, secure image transmission.

I. INTRODUCTION

Nowadays to get a secure system we have to work really hard. Security has been always hard to achieve as the hackers, invent new attacks every day. To protect our personal data in a day to day life has become a huge challenge .sensitive information is hard to be transformed using the medium of internet. Internet as we say is the network of networks that is easily available to everyone. .In recent years, with the evolution of computer and Internet technology, images are widely used to convey information. The wide usage of images in various applications includes medical systems, confidential military archives, enterprises and storage systems. Security is the major issue while transmitting images through internet where hacking of confidential data may take place.Two commonly used methods are data hiding and encryption, decryption method. Information hiding includes watermarking, anonymity and steganographyEncryption of multimedia data can be the immediate solution to protect information against unauthorized access. Such type of techniques required encryption of the data through some sort of mathematical tools where only the actual party that shares the data could possible decrypt to use the data. Encryption uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form. Images are widely used in different-different processes. Therefore, the security of image data from unauthorized uses is important. Image hiding or encrypting method and algorithm can be very from simple methods to more complex and reliable frequency method. Most of the encryption algorithms which are available mainly used for text data and cannot be suitable for multimedia data such as imagesSteganography is actually the science of hiding information from people who would snoop on you. The difference between this and encryption is that the would-be snoopers may not be able to tell there's any hidden information in the first place. As an example, picture files typically have a lot of unused space in them. This space could be used to send hidden messages. It is not, however, true encryption though it can still be quite effective method, and as such, we only mention it here for completeness.Steganography is a technique to hide information from the observer to establish an invisible communication. This steganography system consists of a cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message. To hide hidden information, steganography gives a large opportunity in such a way that someone can't know the presence of the hidden message and thus they can't access the original message.Steganography is the art of concealing a message in a cover without leaving a remarkable track on the original message. Steganography is a technique to hide information from the observer to establish an invisible communication. This steganography system consists of a cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message.

II. LITERATURE REVIEW

Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding. Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion and

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
NCRTET-17
National Conference on Recent Trends in Engineering & Technology
Government Polytechnic College Kasaragod, Kerala
Vol. 4, Special Issue 1

diffusion properties. The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has the correct key. However, the encrypted image is a meaningless file, which cannot provide additional information before decryption and may arouse an attacker's attention during transmission due to its randomness in form. An alternative to avoid this problem is data hiding that hides a secret message into a cover image so that no onecan realize the existence of the secret data, in which the data type of the secret message investigated in this paper, is an image. Existing data hiding methods mainly utilize the techniques of least significant bit substitution, histogram shifting, difference expansion, prediction-error expansion, recursive histogram modification, and discrete cosine/wavelet transformations. If one wants to hide a secret image into a cover image with the same size, the secret image must be highly compressed. One of the compression methods where JPEG compression but it is not suitable for line drawings and textual graphics .Cryptography is widely used and is not a new scenario toa person from computer background. But for a person not from computer background will find it very difficult to send personal images using the concept of cryptography. Cryptography is basically used to hide the original data into a coded data so that unauthorized access can be prevented.

1.1. Transmission techniques

1.1.1. Digital Image Encryption Approach

Everyday technology is changing and according to that; the security norms should also change to keep confidentiality while transmitting. One such approach is Image Encryption, which normally uses the properties and characteristics of digital images to meet the practical requirement in applications related to important fields like medicine and military. The idea behind the image encryption is to create an image with necessary secret data in it, But it is difficult to understand the mechanism behind it. The original image characteristics are considered and converted into the desired security norms. The reliability of the image encryption technique is: No authenticated person can ever decrypt the hidden data without Military Online Confidential Confidential Medical Databases Personal Archives Archives Databases 3 the authenticated key and having the proper knowledge about the desired security norms. Digital image comprises of different properties, and the image encryption approach uses some unique properties of the image to hide the confidential data in digital content in a reliable way. The digital image used in many applications should maintain the security levels in an accurate way to provide better security to the image utilized in the digital media. To accomplish the task of encryption in a reliable way to online storage applications, this is categorized into three groups as following: a. The encryption algorithm based on the position permutation b. The encryption algorithm based on valuing transformation c. The encryption algorithm based on perceived data transformation.An alternative method to avoid this problem is the data hiding that hides a secret message into a cover image so that no one can realize the existence of the secret image. But the main issue of data hiding is that if one wants to hide a secret image into a cover image with the same size, the secret image must be exceptionally compacted ahead of time. However for many applications, such as transmitting medical pictures, legal documents, and military images and so on that contain confidential information, in such cases data compression operations results in a loss of important information.

1.2. Digital Image Covering up Approach

The image encryption has the drawback of natural prediction. The covering upimage. To recover, one must first successfully crack the mysterious element place in the image that is going to be transmitted.Image encryption uses the image default procedures such as high redundancy and bettercorrelation nature in terms of spatial domain. The default properties used for processing depend on Shannon diffusion as well as confusion properties. The secret encrypted image is a noisy image, and it is not revealed until and unless one has the authentic key. The main drawback of the image encryption approach is that it attracts the authenticated person's attention towards it while transmission using the Internet as a source of the medium.Mosaic image is a one type of art in which it is manufactured by generating small pieces of materials like stone, glass, tile etc

1.3. Mosaic Images Transmission Technique

A new technique for secure image transmission is proposed, which transforms a secret image into a significant mosaic image with the same size and resembling a preselected target image. The transformation process is controlled by a secret key and only with the secret key can a person recover the secret image nearly without any loss from the mosaic image. The new strategy is enlivened by Lai and Tsai [4], in which a new sort of computer art image, called secret –

fragmentvisible mosaic image was proposed. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image which is preselected from the database. But an obvious inadequacy of Lai and Tsai [4] is that it requires a large amount of database so that the created mosaic image should be sufficiently similar to the previously selected target image. Using their method the user is not allowed to pick energetically his/her adored image for use as a target image. Therefore in this technique it is desired to remove this weakness while keeping its benefits that is it is aimed to design a new technique that can transform the secret image into a secret-fragment-visible mosaic image of same size that has the same visual appearance of any freely selected target image without the need of a database. A mosaic image is the process of creating pictures or decorative patterns by cementing together small pieces of stone, glass or other hard materials of various colours. Mosaic contains more number of small images called tile images. Mosaic image can be created by dividing the original image into many tiles and for each tile, find another image with similar content from an image database. Finally we have to build the mosaic image by replacing all tiles by their similar images.

III. CONCLUSION

There are so many technique to make an image secure. Some of the encryption techniques used selective part of an image for encryption and some others apply encryption algorithm on whole image bit by bit.The best way of fast and secure transmission is by using compression and encryption of multimedia data like images .Image encryption is a method that makes utilization of the characteristic property of an image, such as high redundancy /repeated information and strong spatial correlation, to get a scrambled image. The scrambled image is a useless document, which can't give extra data before unscrambling and may stir an assailant's attention during transmission because of its irregularity in structure.In mosaic based image transmission, obtained mosaic image, which is identical to the cover image and used as disguise of secret image, is obtained by segmenting the secret image into tiles and their color characteristics are transformed to that of the cover image blocks. Noise may affect the mosaic image while transmitting it to destination in free space.

ACKNOWLEDGMENT

The author would like to express her gratitude to Head of the Institution for constant support and motivation to prepare the paper. Also like to thank Head of the Department and Colleagues and family members for the encouragement.

REFERENCES

[1]G. Chen,Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solit. Fract., vol. 21,no. 3, pp. 749–761, 2004.
[2] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," Chaos Solit. Fract., vol. 24, no. 3,pp. 759–765, 2005.
[3] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," Chaos Solit.Fract., vol. 32, no. 4, pp. 1518–1529, 2007.
[4]. I. J. Lai and W. H. Tsai, "secret-fragment-visible mosaic image-A new computer art and its application to information hiding," IEEE Trans. Inf. Forens. Secur., vol. 6, no. 3, pp. 936-945, Sep. 2011.
[5]http://www.eclipse.org/downloads/packages/release/Galileo/SR2
[6]http://www.ijater.com/Files/5925cf87-315a-47cf-a008-af29f7373f37_NCET_01_02.pdf[7]http://www.ijser.org/researchpaper/Real-Time-Vehicle-License-Plate-Recognition-Based-on-2D-Haar-Discrete-Wavelet-Transform.pdf

Mrs.Neena.M.K, Lecturer in Computer Engineering, Govt.Women's Polytechnic College Nedupuzha, Thrissur,Kerala,India. She Worked as Lecturer in several institutions in kerala. She graduated in Computer Engineering from Model Engineering college, Kochi .She took MTech in ComputerScience from Kerala University in 2009