Study on generating secret image by cryptography and steganography technique for multimedia data transmission

Rahul Mishra, Vinay Gupta

***Abstract-* Data Encryption technique is widely used to ensure security through network. Various types of encryption techniques are used to protect confidential information. In this research paper the visual steganography & Cryptography technique is proposed to transmit multimedia data. This paper proposes a steganography & Cryptography scheme based on the probabilistic model. Here secret sharing scheme is used, where a secret image is encoded into transparencies and random transparencies reveals the secret image. Any information cannot be extract by dealing certain transparencies. The proposed technique provides dynamic change in order to include new transparencies without changing the shape of original transparencies. Proposed work is implemented in MATLAB software. Original image was retrieved successfully at receiving end. Result shows acceptable quality**

Index Terms- Cryptography, Steganography, Information

Objectives-

1- To provide Cryptography & Steganography scheme to transmit multimedia data in channel
2- To retrieve the original image at receiving end
3- To evaluate the effectiveness of proposed work by comparing other exiting techniques

Literature Review

Security Improve in Image Steganography using DES

Authors: M. Ramaiya and N. Hemrajani

The incredible evolution of Internet technologies & its applications require high level the security of data over the communication channel. Image steganography is a digital technique for concealing information into a cover image. Least Significant-Bit (LSB) based approach is most popular steganographic technique in spatial domain due to its simplicity and hiding capacity. All of existing methods of steganography focus on the embedding strategy with less consideration to the pre-processing, such as encryption of secrete image. The conventional algorithm does not provide the preprocessing required in image based steganography for better security, as they do not offer flexibility, robustness and high level of security. The proposed work presents a unique technique for Image steganography based on the Data Encryption Standard (DES) using the strength of S- Box mapping & Secrete key. The pre processing of secrete image is carried by embedding function of the steganography algorithm using two unique S-boxes. The pre processing provide high level of security as extraction is not possible without the knowledge of mapping rules and secrete key of the function. Additionally the proposed scheme is capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption.

Methods of steganography

Steganography methods can be classified mainly into six categories, although in some cases exact classification is not possible.

1. Substitution methods substitute redundant parts of a cover with a secret message (spatial domain).
2. Transform domain techniques embed secret information in a transform space of the signal (frequency domain)
3. Spread spectrum techniques adopt ideas from spread spectrum communication.

Input Design

From the study of the previous research there are many points are noticed that can make un-efficient or imperceptibility of an algorithm. The secrecy, since the strength of earlier algorithm lies in its ability to be noticed by the human eye.

The moment where user/hacker can see that information/image has been tampered with, the algorithm is compromised. Unlike watermarking, which needs to embed only a small amount of copyright information, earlier steganography in other hand requires lots of embedding capacity. Need to improvement in the field of steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganography algorithms leave a signature when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganography algorithm must not leave such a mark in the image as be statistically significant. Need to improvement toward image manipulation, like cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message/image is embedded, these manipulations may destroy the hidden message. It is preferable for steganography algorithms to be robust against either malicious or unintentional changes to the image. With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful existing algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image. Efficiency of the algorithm that means how much efficient in terms of time and how much efficient in terms of memory. Time and memory both are play an important role in efficiency. Security is the prim concerned in the field of encryption. It known that information over public network should be highly secured otherwise any eavesdropper can be easily access information. Encryption Key is play an important role in the field of encryption and security of the algorithm is depending upon key length. Higher key length will be causes higher security. “Error find per execution” that means in single execution how much error have noticed.

Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system’s relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the
- ❖ Future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.

System Analysis

1 Existing System

In Steganography and cryptography, the decoding process is performed directly by the human eyes; while in existing, the shared images need some processing to reconstruct the secret image. The increasing numbers of possibilities to create, publishes, and distribute images calls for novel protection methods, new sharing and access control mechanisms for the information contained in the published images. Secure image sharing techniques overcome the traditional cryptographic approach, providing new solutions for the development of new and secure imaging applications.

2 Proposed System

First, we selected the secret image then selecting the cover image on GUI . Then select Stego base results show up on the base paper. This stego base produces peak-to-signal ratio, entropy and the correlation of secret and cover images. After that, select the Stego Proposed system then we get comparision between the peak-to-signal ratio, entropy and the correlation received results.

Result Analysis

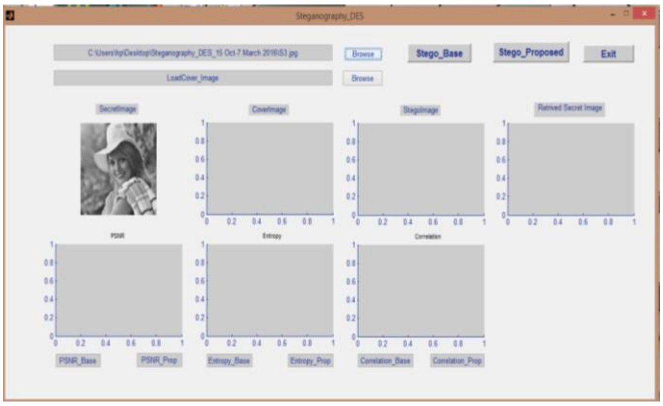
C:\Users\hp\Desktop\Steganography_DES_15 Oct-7 March 2016\S3.jpg
LoadCover_Image

Fig.1: Selecting Secret Image

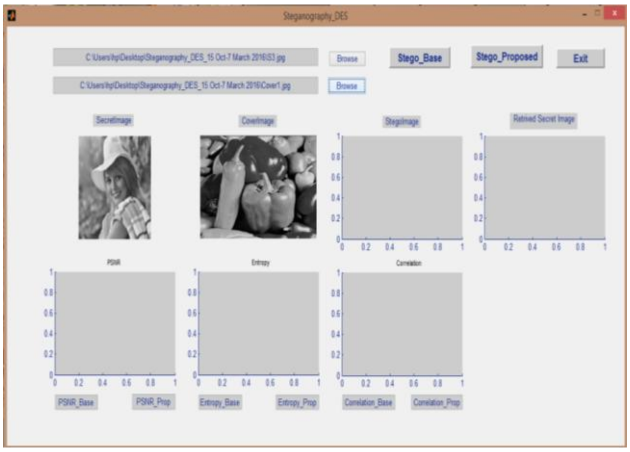
C:\Users\hp\Desktop\Steganography_DES_15 Oct-7 March 2016\S3.jpg
C:\Users\hp\Desktop\Steganography_DES_15 Oct-7 March 2016\Cover1.jpg

Fig.2: Selecting Cover Image

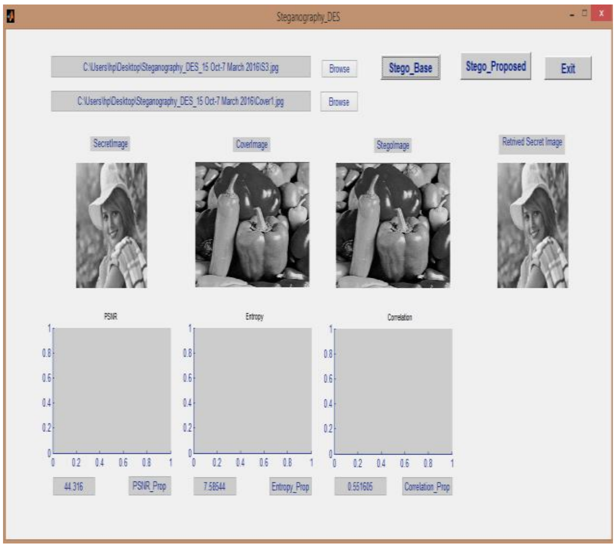
C:\Users\hp\Desktop\Steganography_DES_15 Oct-7 March 2016\S3.jpg
C:\Users\hp\Desktop\Steganography_DES_15 Oct-7 March 2016\Cover1.jpg
44.316
7.58544
0.551605

Fig. 3: Stego base Image Result

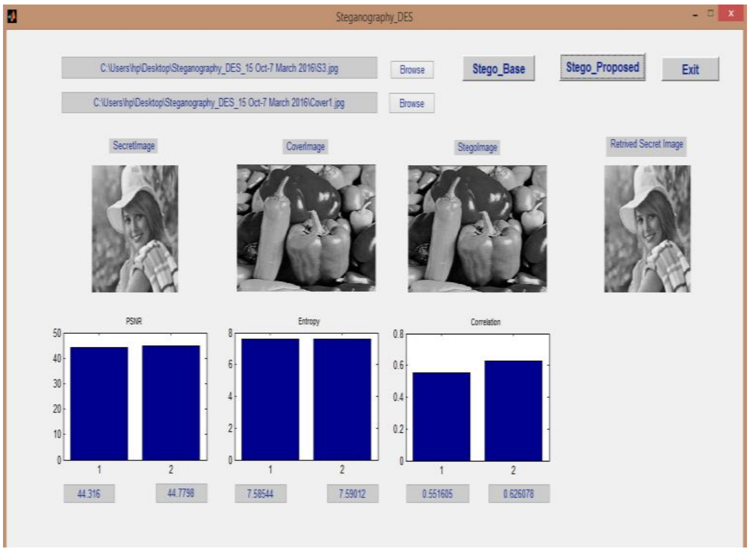
C:\Users\hp\Desktop\Steganography_DES_15 Oct-7 March 2016\S3.jpg
C:\Users\hp\Desktop\Steganography_DES_15 Oct-7 March 2016\Cover1.jpg
44.316
44.7798
7.58544
7.59012
0.551605
0.626078

Fig. 4: Final Result of Proposed system

Conclusion

This work proposed a novel security technique for image as a steganography technique for unseen image files in cover images. Here we have also used a concept of cryptography technique and random number generation during steganography. So form this concept overall security of proposed technique is improving. In this proposed technique, initially cryptography technique applied on secret image and followed by steganography technique with random number generation technique. During results, we have selected some secret images with cover image to be concealed and accomplished that the resultant stego images do not have any perceptible changes. Also we founded good picture quality of the stego images in terms of (PSNR). Proposed technique works highly efficiently. Hence this novel steganography technique is robust and easy to understand. Protection or security from superfluous type sources has become a component of the proposed research work.

References

[1] M. Ramaiya and N. Hemrajani, "Security Improvisation in Image Steganography using DES", IACC IEEE 2013.

[2] Mohammad Shirali-Shahreza , "A new method for real time steganography", ICSP 2006 Proceedings of IEEE.

[3] Yuk Ying Chung, fang Fei Xu , "Development of video watermarking for MPEG2 video" City university of Hong Kong ,IEEE 2006.

[4] C. Lu, J. Chen and K. Fan, "Real-time Frame-Dependent Video Watermarking in VLC Domain", Signal Processing : Image Communication 2005, pp. 624–642.

[5] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual cryptography for general access structures," Inf. Computat., vol. 129, no. 2, pp. 86–106, Sep. 1996.

[6] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38, Mar. 2010.

[7] Z. Zhou, G.R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[8] Z. Wang, G.R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[9] F. Liu, C.K. Wu, and X. J. Lin, "Colour visual cryptography schemes," *IET Inf. Security*, vol. 2, no. 4, pp. 151–165, Dec. 2008.