Enhancement of Security of Digital Data with Steganography Technique

Arpana Bharani
Research Scholar,
Sri Satya Sai University of Medical Science,
Sehore, India

Dr. Jitendra Sheetlani
Dean of Computer Application, Associate Professor
Sri Satya Sai University of Technology & Medical
Technology &
Science, Sehore, India

Abstract: In this era of Internet and Technology there is a need to secure digital data from unauthorized users. This can be done with the use steganography techniques. The selling of softwares in the form of digital images and video sequences is very much enhanced due to the cost effectiveness and improvement in technology. But this digital are also at risk to accidental attacks. Nowadays the most important concern is the protection of digital data and therefore it is gaining interest among researchers. The storing and transferring of digital data, needs many security concerns that are sensitive and if this data is lost, counterfeited, or hacked, it may be impossible to recover. The security of this transmitted data can be increased by the application of steganography techniques. In this the digital data can be hidden in the host image and this image is transferred to the receiving end instead of the actual software data. Then by using a secret key, the hidden data are extracted accurately from the carrier image. The data is hidden in such a way to minimize the degradation of actual data. In this paper a method is described to handle attacks on the carrier image.

Keywords: *Digital data, Steganography, Carrier image*

*****

I. Introduction

With the growth of internet and technology in our day to day life the new business, scientific, entertainment and social opportunities in the form of electronic publishing and advertising, messaging, real-time information delivery, data sharing, collaboration among computers, product ordering, transaction processing, digital repositories and libraries, web newspapers and magazines, network video and audio, personal communication and lots more are being explored with the world wide web [1]. All these applications make use of digital data in form or the other. This digital data can be communicated without comprising quality through data communication networks in a fast and inexpensive way. The digital data can be edited easily as one can access the exact discrete locations where changes are to be made. Also this can be copied easily and copied material is same as original one. The transmission of digital data over the internet very much increases the risk of data being copied. The enforcement of copyright law and verification of content is very difficult in case of digital data. The solution is to use some type of encryption techniques to restrict the access to the digital data. However the encryption does not guarantees the full security. Once the encrypted data are decrypted it can be freely distributed or manipulated.

The solution to the above problem can be done by using some form of hiding the data by some image which can be extracted later to prove the ownership. This can be achieved by data hiding techniques as steganography. The Steganography is the technique of hiding the data in another medium. The cover medium has no relationship with the data or information hidden. The key issue in a steganography system is that no one suspects that a particular medium is carrying any hidden data or information.

II. LITERATURE SURVEY

C.Y. Lin et.al., [2] proposed a method for image authentication that can prevent malicious alteration but allow JPEG lossy compression. The authentication in their method is based on invariance of relationships between discrete cosine transform coefficients at the same position in separate blocks of an image.

Macq and Quisquater [3] in their paper described the issue of watermarking of the digital images with a general survey on cryptography and digital television. The authors presented a description of process to insert a watermark into the least significant bits of pixels located in the vicinity of image contours. In their method the watermark can be easily destroyed as it depends on the modifications of the least significant bits.

Voyatzis G. and Pitas I in [4] describes a method to embed a binary watermark image in the spatial domain. In a spatial transform each pixel of the watermark image is mapped to a pixel of the host image. In their method “toral automorphisms” is used to achieve the chaotic spread of watermark image pixels in the host image.

Lu et al. [5] presented a new watermarking technique called as "Cocktail Watermarking". In this technique the dual watermarks are embedded which are complementing each other. Several attacks are applied resistant to this method and the authors found that this method is resistant to many attacks.

Q. Cheng et.al.[6] presented an suvey on robust optimum detection of multiplicative watermarks. In this the novel optimum detectors for multiplicative watermarks are derived using locally optimum detection for the generalized Gaussian distributions

III. Problem Statement

There must some steganography technique that is more robust and efficient. This steganography technique must be such that it is resistant to various structural and statistical attacks without comprising the quality of image. It must be such that it is difficult for the unauthorized user to find out the difference between the host image and the embedded image.

IV. Proposed Solution

The proposed method improve the robustness of the steganography technique without comprising the quality of the image. Furthermore this proposed method is able to protect the watermarked image even after the cropping attack is applied. In the proposed system the steganography encoding method is used to embed the image onto the original data. This steganography encoding method is resistant to various attacks and it also maintains the quality of the image. After transmitting the data over the communication networks, at the receiving end the steganography decoding method is used to decode the digital data.

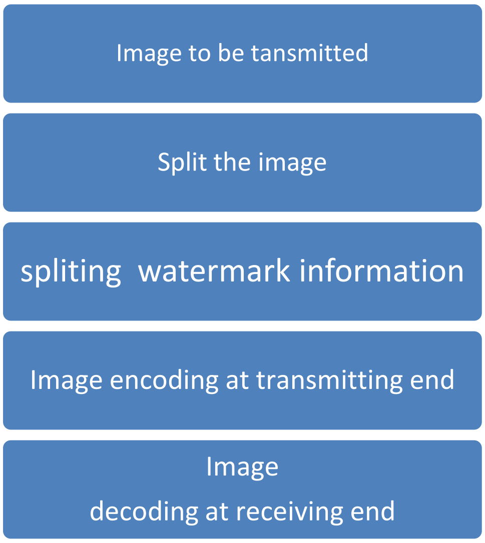
Image to be tansmitted
Split the image
spliting watermark information
Image encoding at transmitting end
Image
decoding at receiving end

Figure 1 : Steps involved in proposed system

Algorithm for the proposed System

START

Step1: Get the original data to be transmitted.

Step 2: Divide the original data into n equal sized frames.

Step 3: Get the watermark image to be embedded.

Step 4: Divide the watermark image into m equal sized pages. (The size of page must be equal to that of size of frame)

Step 5: Calculate the size of original data into bytes.

Step 6: Calculate the size of watermark image into bytes.

Step 7: Divide size of original data and size of watermark image by four. Now we have splitted data and splitted watermark image of same size.

Step 8: Now start with 4 bytes of image, encode 4 bytes of message into that using left/right shift bit operation.

Step 9: Repeat the same technique with the remaining bytes of image.

Step 10: Read all encoded image and merge into final image.

Step 11: Transmit the image.

Step 12: For decoding at the receiving end read first 4 bytes of image and decoded the message using right/left shift bit operation.

Step 13: Repeat the same technique with the remaining bytes of the message.

END

V. Mathematical Model

Let S be the system in which I be the original image to be transmitted and W be the watermark image to be inserted into the original image and E be the extracted watermark image. The I is splitted into n frames, W is also splitted into same sized pages as frames.

S= (I, W, E)

Where S= system, I= Original Image, W= Watermark Image, E=Extracted watermark image.

Input

I = Original Image

W= Watermark Image

Split the original image I = ($I_{1,}$ $I_{2,}$ I_3 ……. I_n)

Split the watermark image W= ($W_{1,}$ $W_{2,}$ W_3……. W_n)

Embeding the image

Embeded Image I_e = (Original Image + Watermark)

Split the embedded image

Extract watermark information

Decode the image

Output

Original watermark information.

VI. Experimental Results

S.No.	Attacks				
1	JPEG Compression	Ratio(%)	10	50	95
		NCC	0.99	0.86	0.71
2	Salt and Pepper Noise	Ratio(%)	20	50	100
		NCC	0.99	0.55	0.53
3	Gaussian Noise	Ratio(%)	10	50	100
		NCC	0.59	0.57	0.55
4	Cropping Attack at various quality levels	Ratio(%)	10	50	75
		NCC	0.56	0.55	0.5
5	Resizing	Ratio(%)	10	50	90
		NCC	0.32	0.54	0.59

VII. Conclusions

The technique used in this research study creates an improved quality of image by embedding the watermark image and this is robust against various attacks like JPEG compression, Noises, Cropping, and Resizing. This method effectively hides the watermark image in the original image that protects the digital data over the communication channel. This protects the digital data from unauthorized access. The system recover the water mark information even though the image is resized by 75%. This method is also useful in transmitting the important data without affecting the quality of original image. The embedded image within the original image can only be recovered by authorized person.

VIII. Future Recommendations

Further research can be done in finding the new technique that promises more robustness against various malicious attacks and provides better image quality.

References

[1] Jain A. K., Uludag U., Hiding Biometric Data, IEEE Trans. Pattern Analysis and Machine Intelligence, 25(11), Nov. 2003, 1494 – 1498

[2] Lin C.Y. et al., A Robust Image Authentication Method DistinguishingJPEG Compression from Malicious Manipulation, IEEE Trans. Circuitsand Systems for Video Technology, vol. 11, no. 2, 2001, pp. 153168

[3] Macq B.M., Quisquater J.J., "*Cryptology for digital TV broadcasting*", Proceedings of IEEE, ISSN**:** 0018-9219, vol. 83, pp. 944-957, June 1995.

[4] Voyatzis G. and Pitas I., "*Digital Image Watermarking using Mixing Systems*", Computer & Graphics, Elsevier, vol. 22, no. 4, pp. 405-416, 1998

[5] Lu C.S., Liao H.Y., Huang M., Sze S.K., *"Combined Watermarking for Images Authentication and Protection"*, Proc. 1st IEEE Int. Conf. on Multimedia and Expo, vol. 3, no. 30, pp. 1415 – 1418, Aug. 2000

[6] Cheng Q. et.al., in [11] presented an investigation on robust optimum detection of multiplicative watermarks. In this the novel optimum detectors for multiplicative watermarks are derived using locally optimum detection for the generalized Gaussian distributions.