International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

Optimized WES-System with Image Bit Embedding for Enhancing the Security of Host Image

Ravikant K[1], Umesh Kumar Lilhore[2]

[1]*MTech Scholar, Dept of Computer Science and Engineering, NIIST, Bhopal, MP, India*
[2] *Associate Professor, Dept of Computer Science and Engineering, NIIST, Bhopal, MP, India*

Abstract - *The protection of intellectual property rights of users became recently a concern especially with the rapid growth of different transmission techniques. In this dissertation, we present a protection method which uses some of the basic techniques for securing data in an image and some other high end methods also. It is a visual cryptographic method which uses watermarking, steganography and an embedded image technique for optimizing the security of host image sent through different transmission techniques. Our methodology uses both image and text watermarking for dismantle the contrast of image, than another image is embedded as a carrier image for more enhancement of security, this image is overlapped with the previous output image. This complete process is taken place at client side and the output of this image is send to the receiver over a transmission medium. The receiver receives the image and applies a set of techniques for extracting the input image and the watermark text if required.*

Key Words: **Watermarking, Steganography, Visual Cryptography, Embedding Image**

1. INTRODUCTION

In the present digital trends of the world, due to the enhanced versions of technologies most of the individuals prefer to use the internet as the primary and major source medium to transfer the information from one point to another point. With the use of internet, data transmission is made very simple and easy to use. Every individual in this world want to save their time for transmission of data from one place to another. However security is the major concern while sending and receiving data over the internet. The private and confidential data can be hacked by unwanted users in many ways.

1.1 Watermarking

Image Watermarking is defined as one of the capable method to eliminate the gap between copyright issues and digital distribution of data between different users. It is primarily based on Steganographic techniques and enables constructive safety mechanisms for images. It is very good standard for copyright issues as it embeds a symbol, a logo or an image in the form of a Watermark, which cannot be altered manually by any unauthorized person. One major factor, which is to be considered while using Watermarking, is to prevent any alterations done to the original image after embedding the data. When image with secret data is transmitted over the internet, unauthorized elements may want to interrupt and hack the data hidden behind the image or want to change it. If the originality of the carrier image has been altered, then it is easier to hack the information by intruders. In order to advance the security, the Digital Watermarks are predominantly inserted as altered digital signal into the original data using key based embedding algorithm and pseudo noise pattern. The best known and commonly used Watermarking method is the spatial domain Least Significant Bit (LSB), which replaces the least significant bits of selected image to hide the information.

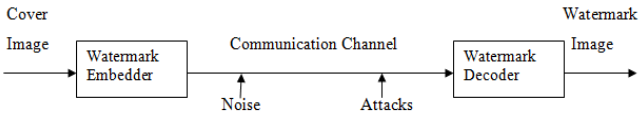

Figure 1: Watermarking Process

1.2 Steganography

Steganogaphy deals with hiding secret data or information within an image. An efficient least significant bit (LSB) technique has been proposed. A spatial domain technique where the secret information which is to be sent is embedded in the LSB position of the cover frames. Eight bits of the secret information is divided into 3,3,2 parts and embedded into the RGB pixel values of the cover frames. A new function is used to select the position of insertion in LSB bits. The proposed method is analyzed in terms of both Peak Signal to Noise Ratio (PSNR) compared to the original cover image as well as the Mean Square Error (MSE) measured between the original and obtained steganographic files. Image Fidelity (IF) is also measured and the results show minimal dreadful conditions of the steganographic image file. The proposed technique is compared with existing LSB method based steganography and the results are found to be cheering. An estimate of the embedding capacity of the technique in the test image file along with an application of the proposed method has also been presented.

1.3 Information Hiding

Information hiding is a recently rapid developed technique in the field of information security and has received significant attention in all the fields. It contains two main branches: digital watermarking and steganography. The watermarking is mainly used for copyright protection of products. While steganography, as a new way of conveying data secretly by concealing the very existence of communication [1]. The carrier for steganography method

can be image, text, audio and video.Image is the most familiar carrier, but the limited size of image will unavoidably restrict the capacity of embedding process. In the case of requiring transmitting large number of secret messages, steganography in image will not satisfy the high demand. Besides, the degradation of image quality cannot be observed only by naked eyes, for it may be aroused by image compression technique of lower quality.

2. THEORITICAL BACKGROUND

There are different types of systems and techniques are implemented for securing the image and data transmission from sender to receiver. Some of the major methods are

2.1 Steganography and its types

a. Fragile: This steganography involves embedding information into a file which will be destroyed if the file is modified by unauthorized user.

b. Robust: Robust marking projects to embed information into a file which cannot easily be destroyed by the intruders.

2.2 Watermarking and its types

a. Image watermarking: In image watermarking techniques the image is used as a envelope to hide the digital data. It is used to protect the photos over the unsecured internet.

b. Video watermarking: In video watermarking the watermark are added to the video segment stream to control the video application. Video watermarking is the higher extension of image watermarking techniques. This method requires real time extraction and robustness for compression of the video.

c. Audio watermarking: This application area is one of the most popular and advance issue due to internet composition of tunes such as MP3.
Text watermarking: This adds watermark to the text file to check the modification made to text files.

d. Graphic watermarking: It adds the watermark image to 2D or 3D computer generated graphics to specify the copyright.

3. LITERATURE REVIEW

Several steganographic methods have been proposed in the past survey and most of which are performed in pixel domain of the images. However major contribution is in the field of domain of Image Steganography, where images are used for watermarking, encryption and covering the original image. The existing methods are mainly based on LSB method where LSBs of the cover image file are directly changed with message bits.
In [1], authors used watermarking technique to provide user authentication in an image by using different images with different sizes.
In [2], authors proposed the encryption of image file using RSA algorithm with quantum computing ideas. After that the encrypted code is included in the cover image which is used to carry the original image. Digital watermark scheme is very important to complete the authenticity of the sender.
In [3], authors proposed a research to increase the message hiding capacity by introducing a new steganography method based on JPEG and quantization table is a continuous process.
In [4], authors exploited the colour decomposition and halftone technology to generate visual cryptograms for both gray-level and colour images. This method can also be easily applied to the schemes developed such as the t out of n threshold scheme and the extended schemes for visual cryptography.
In [5], authors developed a secret sharing visual cryptography scheme of enveloping technique where the secret information are enveloped within other covers mediums of digital pictures using LSB replacement digital watermarking. This adds security to visual cryptography technique from unwanted attack as it befools the hackers' eye.
In [6], authors proposed the extended visual cryptography scheme for natural colour images. Next it showed a method to improve the image quality of the obtained output by enhancing the contrast of the image beyond the constraints. The method enables the contrast enhancement by extending the concept of error and by performing halftoning and encryption simultaneously.
In [7] author has given a robust image steganography technique based on the LSB insertion and RSA encryption technique.
In [8], author has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information.

4. PROBLEM IDENTIFICATION

The past systems were unable to provide high resistance to the high intruder attacks, therefore a new system should me developed inorder to resist these attacks.
Method 1: Only watermarking was used for authenticity of users.
In the initial phase of the security system only watermarking was used to check the authenticity of user. A watermark text or image is embedded into the original image and send it to the receiver. Once the receiver receives the image he/she retrieves the image and extract the watermark embedded into the system. If the watermark received is same as the watermark of the sender than the image is verified.
Method 2: Only steganography was used for hiding the original image.
After the use to watermarking, there was an issue which was still not reduced by the system. By watermarking authenticity is proved but the original image can me exposed to the intruder which makes easier for the hacker to see the original message which is sent by the sender.

Method 3: Combined system with both steganography and watermarking.
This dual system helps to overcome the above two methods but now a day's many high level intruders have different techniques to hack the image or the text transmitted. Again this system lacks in some of the fields. Even after the LSB method used with this system, the data is still not completely secured.

5. PROPOSED METHODOLOGY

Our proposed methodology will try to overcome the problems which encountered in past system and make a secure system for the transmission of data with the use of steganography, watermarking, encryption and image bit embedding for more secure transmission.

Proposed Algorithm

Sender Side Algorithm

1. The INPUT IMAGE is selected, which is to be transmitted.
2. Embed another image as WATERMARK IMAGE into the INPUT IMAGE.
3. Insert TEXT into the WATERMARKED IMAGE for more enhance security.
4. Now encrypt the RESULTANT IMAGE obtained after watermarking using RSA algorithm.
5. Hide the ENCRYPTED IMAGE obtained in step 4 into a carrier image using Steganography.
6. Display the result in the form of "STEGO" image.

Receiver Side Algorithm

1. Select the STEGO image obtained after the sender's process.
2. Extract the hidden encrypted image from the STEGO image.
3. Decrypt the IMAGE using RSA algorithm.
4. Extract the WATERMARK IMAGE and the WATERMARK TEXT which proves the authenticity of the sender.
5. Generate the original image which sender has sent.
6. Display the RESULT.

Comparison Parameters

Peak Signal to Noise Ratio

$$PSNR = 10 \log_{10}\left(\frac{R^2}{MSE}\right)$$

Mean Square Error

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

6. IMPLEMENTATION AND RESULTS

The implementation of this project is done using Matlab and Visual Studio 2008. Five input images are taken of different dimension and size and performed our analysis.

Table -1: PSNR and MSE of different Images

S.N	IMAGE DIMENSION	WATERMARKED IMAGE WITH NOISE		WATERMARKED IMAGE WITH WES SYSTEM	
		MSE	PSNR	MSE	PSNR
Input-1	300*300 (37kb)	0.4021	30.6882	0.4549	38.8745
Input-2	450*450 (39kb)	0.40392	33.6774	0.39608	45.0502
Input-3	600*600 (53kb)	0.2549	32.1041	0.23529	46.3572
Input-4	800*800 (84kb)	0.3594	34.6026	0.34118	49.5581
Input-5	1000*1000 (747kb)	0.45882	37.1966	0.44812	50.3322

From the above table we have analyzed that our WES system is better than normal watermarked system as it gives high PSNR value than watermarked image with noise extraction.

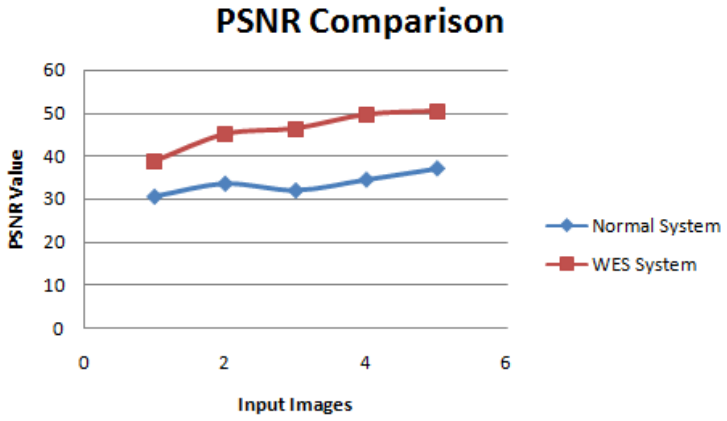

Chart -1: PSNR Comparison

The above table shows the PSNR value of proposed Optimized WES system is more better than simple watermarked image with embedded noise. As by the Matrix Labs, the higher the PSNR, the better the quality of the compressed, or reconstructed image.

3. CONCLUSIONS AND FUTURE SCOPE

We proposed a reduced distortion algorithm for enhancing the image protection. The key idea of the algorithm is using Watermarking, Encryption and Steganography which helps the system to more secure the image transmission. The improvement in presence of additive noise is very much obvious, as the proposed algorithm obtains significantly

lower bit error. The steganalysis of the proposed algorithm is more challenging, because there is a significant number of bits flipped for the data hiding.
A secured LSB technique for Image steganography has been implemented in this project. This technique utilizes cover image files in spatial domain to overcome the presence of sensitive data. Performance analysis of the proposed technique is very much encouraging. Many other techniques are being proposed and some are very much effective also. But our proposed algorithm gives all the three parameters which are required for a secure transmission. It gives Security in terms of encryption, Authenticity in terms of watermarking and Data Hiding in terms of steganography. The future work can be done with other algorithms which are more secure and unaffected from attacks for the encryption of image and also time required for encryption of data.

REFERENCES

[1] Ruchika Patel, Parth Bhatt,"A review paper on Digital Watermarking and its techniques", International Journal of Computer Application, Vol. 110-No.1, Jan 2015.

[2] Hend A. Elsayed,"Image Security Using Quantum RSA Cryptosystem Algorithm And Digital Watermarking", 2016 Progress in Electromagnetic research symposium (PIERS), Shanghai, China, 8-11 August, IEEE 2016.

[3] Shavata Mahajan, Arpinder Singh,"A Review of method & approach for secure Steganography, International Journal of Advanced Research in Computer Science and Software Technology, Vol 2, Issue 10, Oct 2012.

[4] Young Chang Hou, "Visual Cryptography for color images." Pattern Recognition 36 (2003), IEEE 2003.

[5] Shyamalendu Kumar, Arnab Maiti,"Visual cryptography scheme for color images using random number generator with enveloping by digital watermarking" International Journal of Computer Science Issues, Vol 8, Issue 3, No. 1, may 2011.

[6] J. Fridrich, R. Du, and L, Meng, Steganalysis of LSB Encoding in Color Images, in Proceedings of ICME 2000, Jul.-Aug. 2000, N.Y., USA.

[7] Fillatre. L, Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, IEEE Transactions on Signal Processing, Volume 60, Issue:2, pp. 556-569, Feb, 2012

[8] Masud K. S.M. Rahman, Hossain, M.L., A new approach for LSB based image steganography using secret key, in Proceedings of 14th International Conference on Computer and Information Technology (ICCIT-2011), pp.-286-291, Dec. 2011.

[9] Hema Ajetrao, Dr. P.J.Kulkarni and Navanath Gaikwad, A Novel Scheme of Data Hiding in Binary Images, in International Conference on Computational Intelligence and Multimedia Applications, Vol.4, pp. 70-77, Dec. 2007.

[10] Sachdeva S. and Kumar A, Colour Image Steganography Based on Modified Quantization Table, in Proceedings of Second International Conference on Advanced Computing & Communication Technologies (ACCT-2012), pp. 309-313, 2012.