ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

A Secure Image Steganography Technique Based on Kekre's Algorithm

Priyanka Jagota[1], Er. Surbhi Gupta[2]

Scholar at Rayat Bahra Institute of Engineering and Biotechnology Mohali, Punjab[1]

Associate Professor at Rayat Bahra Institute of Engineering and Biotechnology Mohali, Punjab[2]

Abstract: The security of data is a critical factor for solving the problem of stealing, modifying and distributing the intellectual properties in an unauthorized way. Steganography can resolve this issue. Steganography is the science of hiding communication in which secret data or message is embedded into a host signal such as video, image and audio. In this paper, we have improved modified algorithm which is based on LSB technique. This improved modified technique has increased the embedding capacity and quality of stego image as compared to the DCT and DWT technique. The simulation results of improved modified algorithms are compared with DCT and DWT which gives us high PSNR value and low MSE values. Thus, it is clear that in proposed algorithm we can embed large images and use one time random password for security purpose. To measure the quality of stegoimage we use parameters such as PSNR, MSE, SSIM, and Correlation.

Index Terms: Steganography, Improved Modified Kekre's algorithm, PSNR, SSIM, MSE, One Time Random Password.

1. INTRODUCTION

Today, security of the information is the main issue in digital communication. To maintain the security of the confidential data there are two techniques used, one is Cryptography and the other is Steganography. These techniques are used to save the data from unauthorized users. Cryptography is the process in which the content of a message is secure whereas in Steganography, the existence of a message is secure. In cryptography the original message is transformed into another form such as cipher text, but in Steganography the originality of the message does not change. Steganography is derived from the Greek word which means "Cover writing" [14]. The steganography process is represented in diagrammatically form in Figure [1].

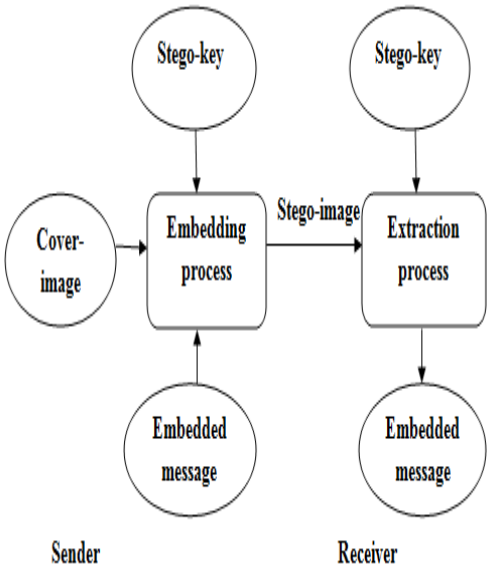

Figure1: Steganography process

In this paper, an improved Modified Kekre's algorithm is being used with the one-time random password technique and compared with the DCT and DWT. The results are evaluated using four parameters such as PSNR, SSIM, MSE and Correlation.

The rest of the work will be grouped into the following sections. Section two comprises of the related work and section three will explain the workflow. Section four and section five will respectively discuss the results and conclusion and future scope.

2. RELATED WORK

Christian and Ramadaniisme [7] explained the methods to hide the secret data into cover image. In this paper, they reviewed various techniques of Steganography in both spatial and frequency domain techniques. Also, they focused in the host documents and various types of images.

Provos et al [1] explained the method to hide secret data into cover image. The authors discussed the existing steganography systems and presented recent research in detecting them via statistical steganalysis. The practical application of detection algorithms and the mechanisms for getting around them were also listed.

Maya et al [3] explained how data hiding was used in bit planes of sub band wavelets coefficients by using the integer wavelets transform (IWT).To increase data hiding capacity while keeping the imperceptibility of the hidden data, the replaceable IWT coefficient areas were defined by a complexity measure used in bit plane complexity segmentation steganography (BPCS). Error control coding was used to reduce the Bit Error Rate (BER) of extracted hidden data when stego image receive some chssannel distortion.

DOI 10.17148/IJARCCE.2015.4998

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Hussain and Hussain[2] introduced a new approach for LSB based image Steganography using secret key to hide the secret message or information into cover image. In this paper, the improved modified Kekre's algorithm is used which increased the hidden capacity of data as well as maintained the quality of image .The improved modified Kekre's algorithm is based upon the LSB(Least Significant Bit). In this the intensity of pixel decided the number of LSB's to be embedded.

Karim et al [4] introduced a new approach for LSB based image Steganography using secret key to hide the secret message or information into cover image. This approach enhances the existing LSB substitution technique to improve the security level of hidden information or message. Depending on secret key hidden information is stored into different positions of LSB of an image. As a result, it was difficult to extract the hidden information or message into cover image. To measure the quality of stego image two parameters PSNR and MSE were used. The value of PSNR gives better result.

Fangjun Huang and JiwuHuang et al [5] explained the rule to hide the secret data into cover image. In this paper, a new channel selection rule was presented for JPEG (Joint photographic experts group (JPEG) Steganography, which can be utilized to find the discrete cosine transform (DCT) coefficients that may introduce the minimal detectable distortions for data hiding. In this paper, three factors were considered in proposed channel i.e. the perturbation error (PE), and the quantization step (QS) and the Magnitude of quantized DCT coefficient to be modified (MQ).

Kevin Curran and Bailey [11] explained that Steganography is the process that involves hiding a message in an appropriate carrier for example an image or audio file. This carrier can is then sent to a receiver without knowing that it contains a hidden message. In this paper, the applications of steganography were also discussed such as civil rights organizations in repressive states to communicate their message to the outside world. It can also be used by terrorists to communicate with one another. The main objectives of this application are to provide the security for the existence of message.

AfrojaAkter et al [8] explained the invisible watermarking, which is also a type of Steganography based on DWT-DCT. This paper, considered a robust image watermarking technique based on DCT and DWT called hybrid watermarking. The hybrid watermarking were performed by two level, three level and four level DWT followed by respective DCT on the host image. A new embedding algorithm of digital watermarking was proposed in this paper. The simulation results were compared with Cox's additive embedding algorithm and the NEA for additive white Gaussian noise attack and without attack. Both algorithms used the hybrid watermarking. The NEA gives better peak signal to noise ratio compared to Cox's additive algorithm for the 4 level DWT for AWGN attack and without attack. So it was conclude that NEA can embed larger marks and high quality marks extract from embedded watermarking even attacked condition.

T.Narasimmalou et al [9] explained a new technique to hide the secret data into cover image. In this paper, an optimal Discrete wavelet transform (DWT) based Steganography was used. First, a single level DWT decomposition was done on a host image and secret information was hidden by manipulating the transform coefficients of the decomposed image. After embedding, the stego-image was subjected to various types of image processing attacks such as Gaussian white noise, salt and pepper noise. Experiments showed that the peak signal noise ratio (PSNR) generated by the proposed method gives the better results.

Laskar et al [10] explained the high capacity data hiding approach by using LSB steganography and encryption to hide the secret data or information into cover image. They explained about the combination of encryption and Steganography. A message was first encrypted using transposition cipher text and then the encrypted message was embedded inside an image using LSB insertion method. The combination of these two increased the security of the secret message. MSE and PSNR were calculated to measure the quality of image .The main objective was to provide resistance against visual and statistical attacks as well as high capacity.

Hussain and Hussain [12] explained that steganography is a process that involves hiding a message in appropriate carrier such as image, audio and video. The carrier can then be send to the receiver without knowing about the secret message. Various types, techniques, terminologies, classifications and applications such as military purpose, medical images were described.

Siwei Lyu and Hany Farid [13] described a universal approach to steganalysis for detecting the presence of hidden messages embedded within digital images. it showed that within multiscale, multiorientation image decompositions, first and higher- order magnitude and phase statistics were relatively consistent across a broad range of images, but distributed by the presence of embedded hidden message. In this paper efficiency had been checked on the basis of large collection of images and on eight different steganography embedding algorithms.

3. PROPOSED ALGORITHM & WORK FLOW

In the purposed work the images have been used as cover object. This secret information have been embedded behind these images using different approaches. In the purposed work the secret information has been hiding behind the least significant bits of the cover object. In this the flow diagram of the proposed work will shown as below in figure 3.

Algorithm

1st phase: In the very first stage, a cover image is selected by the user from the dataset.

2nd phase: In the second stage, a secret image is selected by the user.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

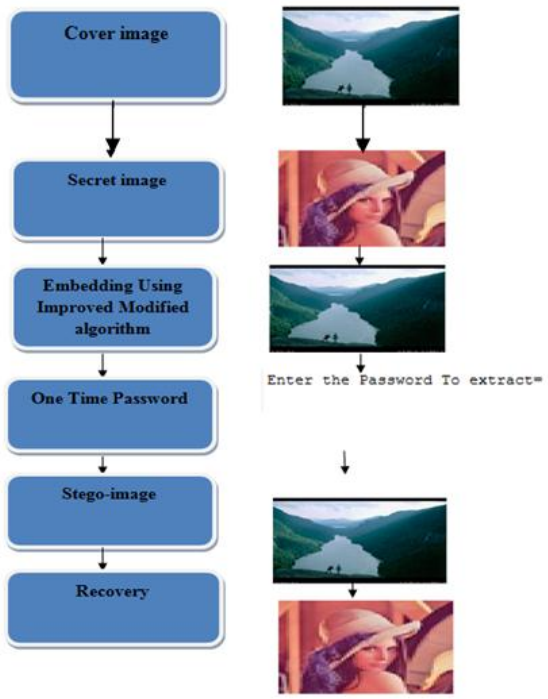

Figure: 3 Work Flow

And then, we calculate the size of secret image.

- If the capacity of the cover image is greater than equal to the message size of the secret image then stego image is represent.
- Otherwise it shows an error that select a another image.

3rdPhase: In the third phase, embedding process is performed by the user:

- In the first step, we divide the cover image into three colors red, green, and blue and also collect the information of its height and width.
- Then, we get the information of the secret image regarding its height width. And hide the secret image of height and width in the cover image of height and width.
- In second step, get the red, green and blue color of the secret image.
- Then convert the secret image into the binary form and set a counter for the pixels.
- In the third step, we embed the red, green and blue part of the secret image in least significant bits of red, green and blue part of the cover image and form stego-image.

4th phase: In the fourth phase, after embedding the following four parameters are calculated: PSNR, MSE, SSIM and Correlation.

5th phase: In the fifth phase, the stego image is selected which is formed in embedding process.

6th phase: In the Sixth phase, the onetime password is generated. With the help of this password, the unauthorized users cannot access the data easily. This password is sent to the e-mail of the receiver by the sender.

- If the OTP which is send by the sender to the receiver in mail is matched with the generated OTP then secret message is extracted easily.
- Otherwise it shows an error.

7th phase: In the seventh phase, secret message is shown which is hidden in the cover image.

Input: Cover Image F & Secret Image G

Output: Stego Image y

Begin

1. Read Cover Image (F) & Secret Image (G) from database
If size (G)> Size (F)
Break
Else
F_R =F (:,:,1) G_R = G (:,:,1)
F_G =F (:,:,2) G_G =G (:,:,2)
F_B =F (:,:,3) G_B =G (:,:,3)

2. P=Generate Random password of between 0 to 999
Password=decimal 2 binary (P)
For F (1, 1) = embed (P, F (1, 1))

3. For i=1 to end
For j=1 to end
HRC=LSB of F_R (I, j) + Gr
Hg=LSB of F_G (I, j) + GG
Hb= LSB of F_B (I, j) + Gb
End for loop j
End for loop i
H=H_R + H_G + H_B
His output image

4. RESULTS & DISCUSSIONS

In this, the embedding used improved modified algorithm and onetime random password. The images which are used in this paper have been taken for database [15].. The quality of the steganography is measured using different parameters that are PSNR, MSE, SSIM and CORRELATION.

In this paper, the results of colored images using improved Modified Kekre's algorithm and OTP (one time random password) are shown in table 4.1. In this the OTP is used as a security purpose through which unauthorized users cannot access the secret data easily.

IM no.	PSNR	MSE	SSIM	CORRELATION
1	42.6	3.72	0.87	0.99
2	39.0	8.60	0.98	0.99
3	38.8	8.93	0.86	0.99
4	39.3	3.58	0.96	0.99
5	41.7	3.54	0.98	0.99
6	41.3	4.66	0.76	0.99
7	39.8	12.32	0.97	0.99
8	40.0	9.58	0.74	0.99
9	39.0	8.78	0.98	0.99
10	38.8	9.23	0.95	0.99

Table 4.1 values of IMKA (improved modified kekre's algorithm) using colored images

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

In this paper, for comparison we convert the RGB images into the gray scale images. In DCT, the grayscale images were used so that's why we convert the images into the gray scale images.

IM no.	PSNR	MSE	SSIM	CORRELA -TION
1	49.3	0.76	0.91	0.99
2	45.1	1.9	0.98	0.99
3	45.41	1.86	0.96	0.99
4	45.05	2.20	0.96	0.99
5	38.25	9.70	0.98	0.99
6	48.25	0.97	0.81	0.99
7	49.31	0.76	0.89	0.99
8	43.60	2.83	0.80	0.99
9	35.36	18.9	0.94	0.99
10	41.91	4.18	0.96	0.99

Table 4.2 comparison values of DCT and DWT using gray scale images.

This table 4.2 represents the values of DCT & DWT using gray scale images. In this table, we measure the quality of stego image using four parameters: PSNR, MSE, SSIM, and Correlation which are given in table.

Im No	PSNR	MSE	SSIM	CORRELA -TION
1	69.60	0.067	0.97	0.99
2	68.68	0.066	0.99	0.99
3	74.76	0.013	0.99	0.99
4	67.15	0.063	0.99	0.99
5	67.76	0.056	0.99	099
6	67.96	0.032	0.99	0.99
7	62.72	0.095	0.98	0.99
8	65.63	0.030	0.98	0.99
9	62.16	0.095	0.99	0.99
10	76.02	0.002	0.99	1

Table 4.3 comparison values of IMKA (improved modified kekre's algorithm) using gray scale images

This table 4.3 represents the values of improved modified Kekre's algorithm using gray scale images. In this table, we measure the quality of stego image using four parameters: PSNR, MSE, SSIM, and Correlation which are given in table.

From this table, it is clear that improved modified algorithm attains better quality rather than the DCT and DWT technique

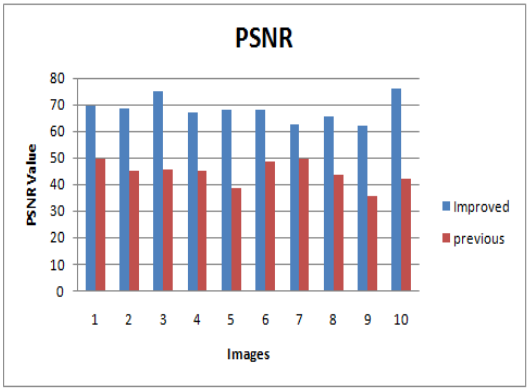

Figure 4.2: Graph for PSNR Values.

This graph represents the difference values of DCT and DWT and proposed work using gray scale images. Higher the PSNR values better the quality of image.

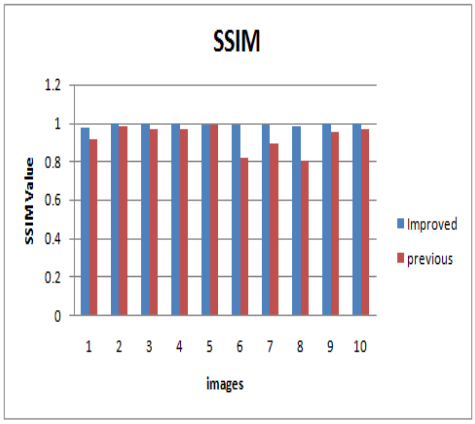

Figure 4.3: Graph for SSIM Values

This graph represents the difference values of DCT and DWT and proposed work using gray scale images.

If the value of SSIM is close to 1 then there are fewer changes in cover image and stego image.

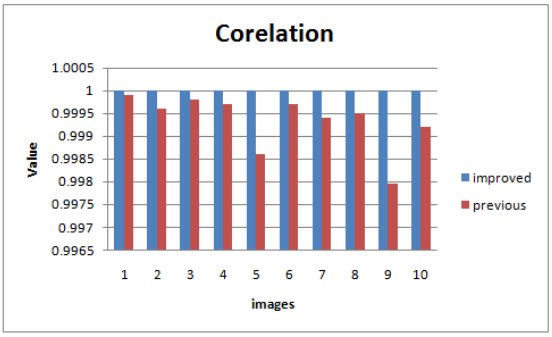

Figure 4.4: Graph for Correlation Values

This graph represents the difference values of DCT and DWT and proposed work using gray scale images.

If the value of Correlation is close to 1 then there is relationship between cover image and stego image.

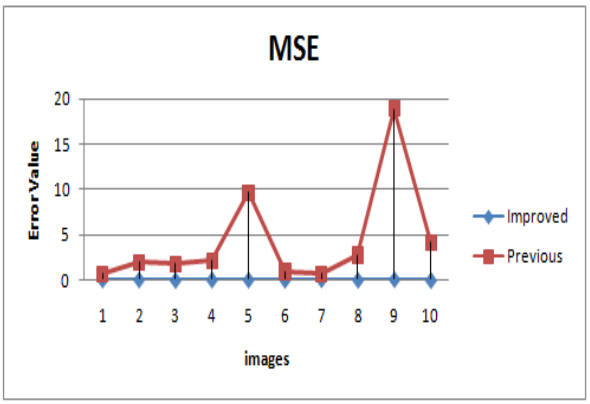

Figure 4.5: Graph for MSE Values.

This graph represents the difference values of DCT and DWT and proposed work using gray scale images. Lowest the MSE value better the quality of image.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

V. CONCLUSION AND FUTURE SCOPE

From the above discussions it is concluded that the proposed technique has better quality of image because its PSNR attains highest value and MSE contains lowest value. And with the help of OTP we maintain the security to the confidential data and through which unauthorized users cannot access the data easily. In future, different security techniques can be used to secure the data.

REFERENCES

1. Provos, N., Honeyman, P, "Hide and seek: An introduction to steganography," IEEE Security & Privacy Magazine 1 (2003) pp. 32-44.
2. Mehdi Hussain, Mureed Hussain "Pixel Intensity Based High Capacity Data Embedding Method", 2010, IEEE.
3. Silvia Torres-Maya, Mariko Nakano- Miyatake and Héctor Perez-Meana *SEPI,"* An Image Steganography Systems Based on BPCS and IWT" 16th IEEE International Conference on Electronics, Communications and Computers (CONIELECOMP 2006), IEEE
4. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key" International Conference on Computer and Information Technology (ICCIT 201 I) Pp. 22-24 December, 2011, IEEE.
5. Fangjun Huang,Jiwu Huang,and Yun-Qing Shi,*"* New Channel Selection Rule for JPEG Steganography" IEEE Transactions on Information Forensics and security, vol.7, no. 4, AUGUST 2012.
6. Alaa A. Jabbar Altaay, Shahrin bin Sahib, Mazdak Zamani "An Introduction to Image Steganography Techniques "International Conference on Advanced Computer Science Applications and Technologies, 2013, IEEE.
7. Ramadhan Mstafa, Christian Bach "Information Hiding in Images Using Steganography Techniques" 2013 ASEE Northeast Section Conference Norwich University Reviewed Paper March, Pp. 14-16, 2013
8. Afroja Akter, Nur-E-Tajnina, and Muhammad Ahsan Ullah "Digital Image Watermarking Based on DWT-DCT Evaluate for a New Embedding Algorithm" 3rd International conference on informatics electronics & vision, 2014, IEEE.
9. T. Narasimmalou, Allen Joseph "Optimized Discrete Wavelet Transform Based Steganography" 2012, IEEE International Conference on Advanced Communication Control and Computing Technologies.
10. Shamim Ahmed Laskar and Kattamanchi Hemachandran "High Capacity Data Hiding approach by using LSB steganography and encryption**"** International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012.
11. Kevin Curran, Karen Bailey" An Evaluation of Image Based Steganography Methods" International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2.
12. Mehdi Hussain and Mureed Hussain "A Survey of Image Steganography Techniques" International Journal of Advanced Science and Technology Vol. 54, May, 2013.
13. Siwei Lyu, Hany Farid,*"* Steganalysis Using Higher-Order Image Statistics IEEE Transactions on Information Forensics and Sceurity, Vol. 1, NO. 1, 2006 IEEE.
14. Mandep Kaur, Surbhi Gupta, Parvinder S. Sandhu, Jagdeep Kaur "A Dynamic RGB Intensity Based Steganography Scheme World Academy of Science, Engineering and Technology 43 2010.
15. Database link: http://wang.ist.psu.edu/docs/related/