ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Multilevel Security for Highly Sensitive Cover Image based on RDH using Histogram Shifting

Ashwini. H.K[1], Dr.Y.C. Kiran[2]

P.G. Student, Department of Computer Science &Engineering, BNMIT, Bengaluru, Karnataka, India[1]

Associate Professor, Department of Computer Science &Engineering, BNMIT, Bengaluru, Karnataka, India[2]

ABSTRACT: The work proposes a Reversible Data Hiding (RDH) scheme for grayscale cover images with highly sensitive cover image. The scheme exploits least complexity in computation by incorporating histogram shifting method to embed secret bit in confused cover, where cover confusion has been implemented using logistic map function. The proposed methods use chaotic encryption to secure cover image which selectively encrypt some of the bits in image using confusion and diffusion methods. Furthermore, extracted information after the decryption is generated along with the unique id, which gives the detailing of the information retrieved at the user end. The method undergoes two level of encryption in order to ensure higher security for the cover image also by using RDH technique original cover can be losslessly recovered after extraction of embedded data.

KEYWORDS: RDH, Histogram Shifting (HS), Chaotic-encryption.

I. INTRODUCTION

With the fast advancement of data innovation, security infringement and copyright validation issues of the mixed media items have turned out to be more genuine. Despite the fact that specialists concocted a lot of arrangements, a solid and additionally an effective route for tending to this issue was steganography.

Steganography is the technique for hiding information/data within the cover content in a credulous manner. The root words of the name steganography were evolved from Greek, “stego” means “covered” or “secret” and “graphy” means to “write” and thus, steganography becomes “covered or secret writing”. The information to be hidden is converted into binary values and embedded into the cover object, which can be a text, some image, or some audio /video file. The processes of data hiding should be well-designed so that the existence of the hidden message is undetected by maintaining the appearance of the cover image exactly the same as original image. The main goal of steganography is to hide the fact that the message is present in the transmission medium.

Starting late, reversible data concealing has drawn various researchers thought. Reversibility grants interesting media to be completely recovered from stego-media after the embedded message is isolated. New methodology which consider spread picture in like manner as an information to transmit securely over framework has introduced as a result recently look into suggestion. So there must be a way to deal with insurance security of spread picture.

II. RELATED WORK

Akhtarv N Johri, et al.[1], proposed a variation of plain LSB (Least Significant Bit) algorithm. The stego-picture quality has been enhanced by utilizing bit-reversal procedure. LSB strategy enhancing the PSNR (Peak Signal to Noise Ratio) of stego picture. Through putting away the bit designs for which LSBs are rearranged, picture might be acquired accurately.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

The introduced strategy indicates great improvement to Least Significant Bit method in thought to security and in addition picture quality.

Manjunatha reddy and Raja et al.[2], proposed High Capacity and Security Steganography Using Discrete Wavelet Transform. The protected information transmission over web is accomplished utilizing Steganography. The wavelet coefficients of both the cover image and payload are intertwined into single picture utilizing inserting quality parameters alpha and beta. The cover image and payload are preprocessed to diminish the pixel reach to guarantee the payload is recovered precisely at the destination. It is observed that the capacity and security is increased with satisfactory PSNR in the proposed calculation contrasted with the current calculations.

Thenmozhi S and Chandrasekaran M et al.[3], presented the novel scheme embeds data in integer wavelet transform coefficients by using a cropping function in an 8×8 block over the cover image. The optimal pixel change process have been applied after embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoids the floating point precision problems of the wavelet filter.

Kirti Gandhi, Gaurav Garg et al. [4], introduced a method which is a variant of so far well-known LSB method. Due to less robustness and max vulnerability to be attacked LSB method is not suitable to prefer. Instead two bits (2^{nd} and 3^{rd} LSB's) are used for hiding message which will increase the data hiding capacity also. The filter is designed such a way that it should minimize the changes occurred in stego file. The stego file along with the filtered file thus obtained is used to generate a unique key. The filtered file and the generated key will be transmitted to receiver. The key will derive to extract the correct message at receiver's end.

III. MODULE DESCRIPTION

- **Pre-Processing**
  This module is the initial stage for work to progress with. Here the image is selected in two ways they are:
  1. Secret Image: This image can be any grayscale image where its pixel value is reized for 128X128 bits.
  2. Cover Image: The cover image is the one which holds secret bits of data so the image here is resized into 1024X1024.

- **Image Encryption and Decryption**
  This module details the working of Multi-level encryption and decryption operation on both sides of the user end and is indecomposable at any point of time as we are using chaotic algorithm to obtain better security than any existing system deals with.

- **Data hiding using HS**
  Fig 1 shows the System Architecture of the proposed system. The Encrypted input image is divided into blocks and then histogram shifting is done on each block which enhances the data hiding capacity and visual quality.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

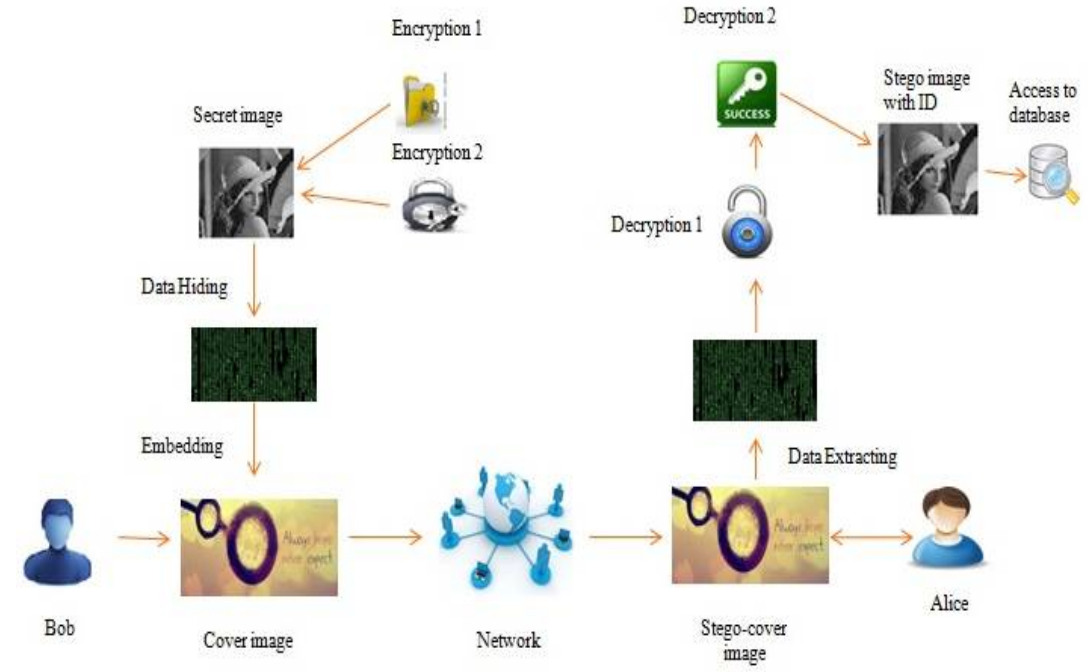

Fig 1: Proposed System Architecture

Fig 1 describes Architecture ofproposed system. Data transmission is made between two users, bob selects the secret image performs the encryption operation which generates the key and is shared, later the encrypted secret image is embedded over cover image and is transformed over network. At the receiver end Alice with decryption key will decrypt the original data along with generated id for further detailed info of obtained image.

IV. CHAOTIC ALGORITHM

Consider an image plaintext *f(i,j)* and key is $k(k_1 ; k_2) = k(\mu^1, x^1_0 ; \mu^2, x^2_0)$ is the initial conditions of two chaotic systems, respectively.

This scheme of encrypting image consists of five steps:

(1) Generate a chaotic sequence using the sub-key k_1 as the initial conditions of the first chaotic system.

(2) Transform the chaotic sequence into a binary stream by a threshold function.

(3) Modify pixel values of the plain image *f(i,j)* using the binary stream as a key stream and get the image $f'(i,j)$. The performing operation is bit-wise XOR.

(4) Construct a permutation matrix P using the sub-key k_2 as the initial conditions of the second chaotic system.

(5) Encrypt the image $f'(i,j)$ by permutation matrix P and get the encrypted image $f''(i,j)$.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

V. EXPERIMENTAL RESULTS

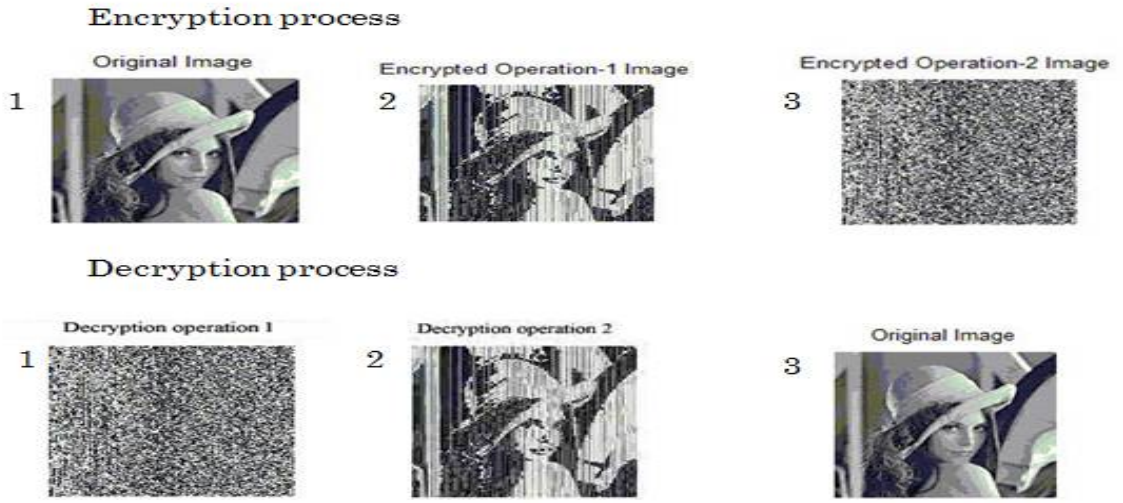

Fig 2: Multi-Level Encryption and Decryption of standard Lena image

Figure 2 from the above experimental results shows various stages of encryption and decryption operation. Using the chaotic encryption standard ,the Lena image undergoes encryption operation. At the very first image is coverted into binary bits which is shown in encryption (fig no.2) using XOR operation, further another level of encryption is performed by changing the pixel ditrortion position which is shown in encryption (fig no.3). During this stage each level of encryption would generate a secret key which is used at receiver end to decrypt the encrypted data. Here the encryption process is performed reverse order in order to obtain secret image over the cover image.

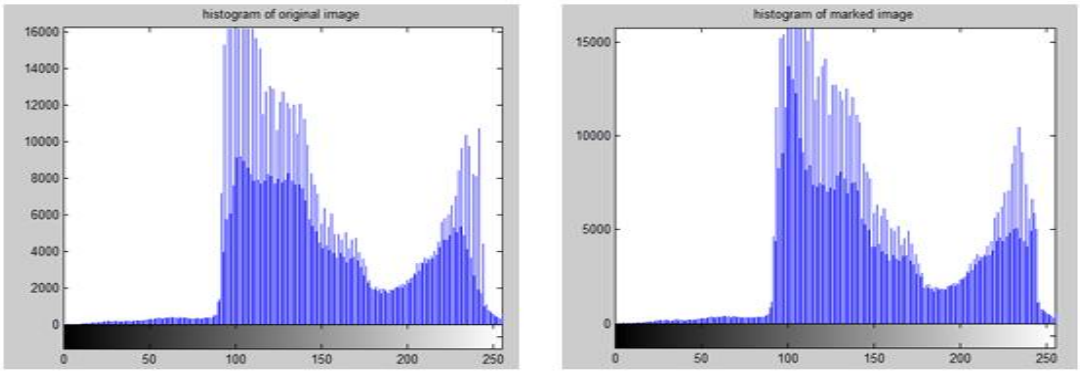

Fig 3: Histogram Difference between original image and data marked(hided) image

Fig 3 shows the Histogram of original image and data embedded image as shown above, where x-axis denotes pixel position and y-axis denotes intensity level of each pixel, which clearly depicts the original cover image

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

and cover image after data embedding wouldn't result in distortion of original image and remains the same at receiver end as well.

The Table 1 below shows the comparative results for various size of standard Lena image. Higher the PSNR(Peak Signal to Noise Ratio) maximum will be the obtained image intensity. That means the recovered secret image is better compared to other results and max intensity is drawn. Normally in any existing system the PSNR would range between 54~60.

Table 1: Comparison results for Lena Image

Carrier Size	PSNR for existing method (dB)	PSNR for proposed method (dB)
2048X2048	53.3	75.4255
1024X1024	52.9	74.4606
512X512	50.5	74.0809
256X256	49.5	73.6560

VI CONCLUSION

In this proposed work, Multi-level security for the secret image which is embedded over the cover image have been studied with intent to find all possible solutions.Usage of technique that is chaotic encryption is used for image encryption security and RDH ensembles the encrypted image over cover content by breaking them into chunks. This method can be applied for any image format which is gray scaled during preprocessing. Further the enhancement would include generating unique ID for each image which gives the detailing of that image at the receiver end. Over all it gives the maximum PSNR value for the obtained image and is effective and more secured than any other existing system.

REFERENCES

[1] Kantar N, Jiri P, and Khan S,"Enhancing the Security and Quality of LSB Based Image Steganography," fifth International Conference on Computational Intelligence and Communication Networks (CICN) pp.385-390, 27-29 Sept. 2013.
[2] H S Manjunatha reddy and K B Raja, "High Capacity and Security Steganography Using Discrete Wavelet Transform", Proceedings of International Journal of Computer Science and Security,pp. 462-472,2010.
[3] S Thenmozhi ,Dr M Chandrasekaran , "Novel methodology for picture stenography in light of whole number wavelet change," International Conference on Computational Intelligence and Computing Research,pp 173-178,ISBN: 978-1-4244-5956-8, 2012.
[4] Kirti Gandhi, Gaurav Garg, "Altered LSB Audio Steganography Approach" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2012, pp 158-161.
[5]Huang-Pei xiao,Guo-Ji Zhang " An image Encryption scheme Based on Chaotic Systems," 5th International Conference on Machine Learning and Cybernetics,Dalian,13-16 August 2006.