Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 4, April 2018, pg.125 – 134

Security Based Image Processing using Reversible Data Hiding Method

Tejaswini H N[1], Chaitra S[1], Soundarya M[1], Monika M M[1], Ms. Ayeesha Siddiqha[2], Ms. Shruthi T R[2]

[1]Final year BE pursuing in Computer Science & Engineering, Malnad College of Engineering, Hassan
[2]B.E, M.Tech Asst Professor, Malnad College of Engineering, Hassan

ABSTRACT: Encryption is a process which uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form. To secure the exchange of important multimedia data over the internet, steganography techniques are extensively used in recent years. By using such techniques the sensitive data is hidden in covert object making its existence imperceptible to the intruder during transmission. In our project we mainly use system Reversible-Data-Hiding method for embedding and extraction of secret image. It depends on the histogram-shifting. We basically have two phase they are embedding phase and extracting phase.

Keywords: Encryption, reversible data hiding, embedding, histogram, extraction.

I. INTRODUCTION

The internet is one of the most powerful creations in all of human history. Internet was started in the earlier days to exchange important information among all the scientists over different colleges and universities and also to provide the information and communication in the medical applications and war field to exchange crucial data. Nowadays internet is being widely used for exchange of information in various fields. Since the beginning of the web, the security and the confidentiality of the vital data have been very important and highest priority. The security and confidentiality of crucial data is needed because if the crucial data is exchanged in the existing communication then many intruders or attackers can be hacking the information. So to exchange the crucial data security and confidentiality is needed.

The security of gray scale image data from unauthorized users is important. Image encryption method prepared information unreadable. Therefore, no hacker or eavesdropper, including server administrators and others, have access to original message. To secure the exchange of important multimedia data over the internet, steganography techniques are extensively used in recent

years. By using such techniques the sensitive data is hidden in covert object making its existence imperceptible to the intruder during transmission.

A grayscale or greyscale image is one in which the value of each pixel is a single sample representing only an amount of light, that is, it carries only intensity information. Images of this sort, also known as black-and-white or monochrome, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest [1].

Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only two colors, black and white (also called bi-level or binary images). Grayscale images have many shades of gray in between.

II. PROBLEM STATEMENT

Security is the most important issue in the process of transmission of gray scale images through Internet. There are many image encryption techniques but they are not that secured. So in our project we try to over-come this problem.

The system should be able to hide a grayscale image in a cover-image with good imperceptibility at the sender. At the receiver, the system should be able to extract the secret-image without any distortion and the original cover-image has to be restored by compensating the changes whatsoever made during embedding the secret-image. Classical steganography concerns itself with ways of embedding a secret message (which might be a copyright mark, a covert communication, or a serial number) in a cover message. The embedding is typically parameterized by a key; without knowledge of this key (or a related one) it is difficult for a third party to detect or remove the embedded material. Once the cover object has material embedded in it, it is called a stego object. Thus, for example, we might embed a mark in a cover text giving a stego text, or embed a text in a cover image giving a stego-image; and so on.

In our project we mainly use system Reversible-Data-Hiding method for embedding and extraction of secret image. It depends on the histogram-shifting. We basically have two phase they are embedding phase and extracting phase. In Embedding phase we first select the secrete image and cover-image then by further process the image will be encrypted by cover-image. And the embedding process is done in reverse. Then the original cover-image is also extracted after extracting the secret data. Finally after completing the extraction process the output is the extracted secret-image and the recovered original cover-image.

III. EXISTING SYSTEM

The resources we obtained are being used without proper security which is leading to insecurity of images. In some techniques we lose our original data at the receiver data which causes a huge loss to both sender and receiver [2], low distortions in image quality. The main concepts we are concentrating on is security, there should be no loss of data at the receiver side.

In a work on [1] RDH system the difference of neighboring pixel values are found and from those values some difference values are chosen for the Difference Expansion (DE). The message confirmation code, original data information and additional information will all be embedded into the difference values. It is an exceptional reversible-data-hiding method regarding low distortions in image quality and high embedding capacity.

In the histogram [3], they find out the peak points, b (p) and b (z). Then the peak point in the histogram will be shifted to right one. So that the pixel value of b (p) is emptied and b (p+1) becomes the new peak point. Then the secret-data bits can be embed into the cover-image. If the secret-data bit '0', then the histogram is shifted and embeds the data. If the secret bit is '1', then it remains same. In the decoder phase, the secret-data and original cover-image will be extracted.

In a RDH system proposed in [4], the contrasts between neighboring pixels are used rather than simple pixel quality in his work on RDH system. Since image neighbor pixels are emphatically connected the difference is expected very near to zero, at the sending side, the image is extracted in an inverse s-order and after that ascertain the pixel difference between x_i-1 pixels and x_i and peak points of histogram are resolved.

Reversible-data-hiding [5] has perspective on modification of histogram and its difference image is created using the linear prediction method. This method is also used multiple times to get high embedding capacity. The embedding process of this method determines the prediction errors to create distinct image from the relationship of the neighborhood pixels and after that embed secret-data bits in to the prediction errors.

A histogram based RDH method is used [6]. The cover-image is divided into number of same dimension blocks and then generates the histogram for every block. Find out the Maximum and a minimum point for these histograms then the space is generated to embed the hiding data bits. By doing this the embedding capacity is decreased but there is great image quality.

IV. SYSTEM METHODOLOGY

A. Image Processing Using Reversible Data Hiding Method

This method is used for embedding and extraction of secret image. As we are encrypting gray scale images which are composed exclusively of shades of gray. First the colour images are converted into gray scale images. It can be done using rgb2gray function. It converts the TrueColor image RGB to the grayscale intensity image. The rgb2gray function converts RGB images to grayscale by eliminating the hue and saturation information while retaining the luminance. If you have Parallel Computing Toolbox installed, rgb2gray can perform this conversion on a GPU.

Then as this method depends on histogram-shifting. To begin with this method the cover image and secret image will be selected and the cover image is divided into non-overlapping blocks. In each block maximum pixel value is selected and difference between the maximum pixel and the remaining pixel is to be found. The difference histogram will be generated and the histogram will be shifted then the secret bits will be embedded. The stego-image which is the output of the embedding process which contains hidden message either in the pixel values or in optimally selected coefficient which is formed and done in embedding phase as shown in the figure 1.

In the receiver side the stego-image will be divided into non-overlapping blocks. Again the same maximum pixel value is selected which was done as in embedding phase, the difference histogram will be generated and shift the histogram back to recover the lower bound pixel and upper bound pixel and extract the secret image bits and also cover image without distortion with high payload.

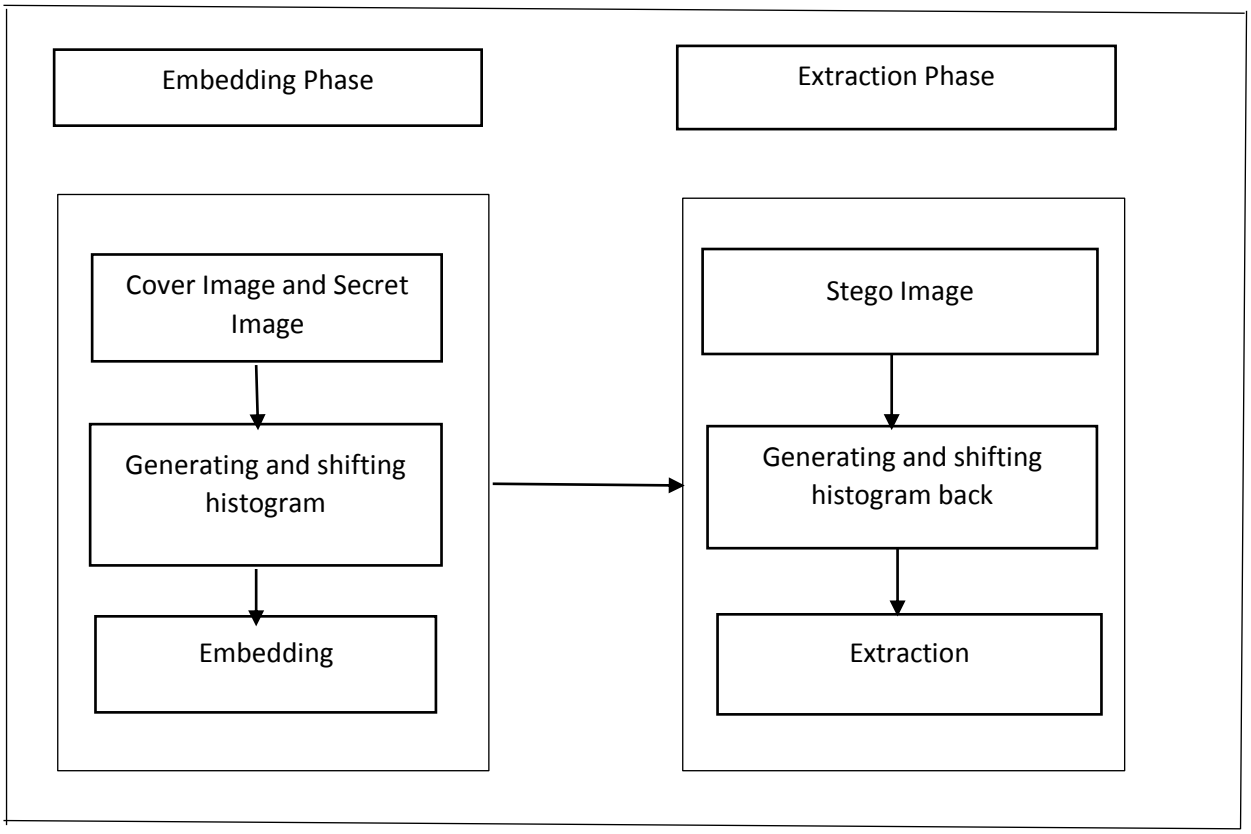

Fig 1: System Architecture

B. EMBEDDING PROCESS

In the embedding process the image will be selected as the cover-image and the cover-image is checked whether the lower bound pixel and the upper bound pixel is 1 and 254 pixel respectively to avoid overflow and underflow problems in the time of embedding.

Cover-image will be divided into non-overlapping blocks and in each block 1 pixel is selected as the reference pixel and the difference between the reference pixel and remaining pixel in the blocks are found. The difference histogram is generated and is shifted for embedding the secret-information is as shown in the figure 2. Histogram is a diagram consisting of rectangles whose area is proportional to the frequency of a variable and whose width is equal to the class interval. A histogram is an accurate representation of the distribution of numerical data. It is an estimate of the probability distribution of a continuous variable (quantitative variable). It is a kind of bar graph. To construct a histogram, the first step is to "bin" the range of values—that is, divide the entire range of values into a series of intervals—and then count how many values fall into each interval.

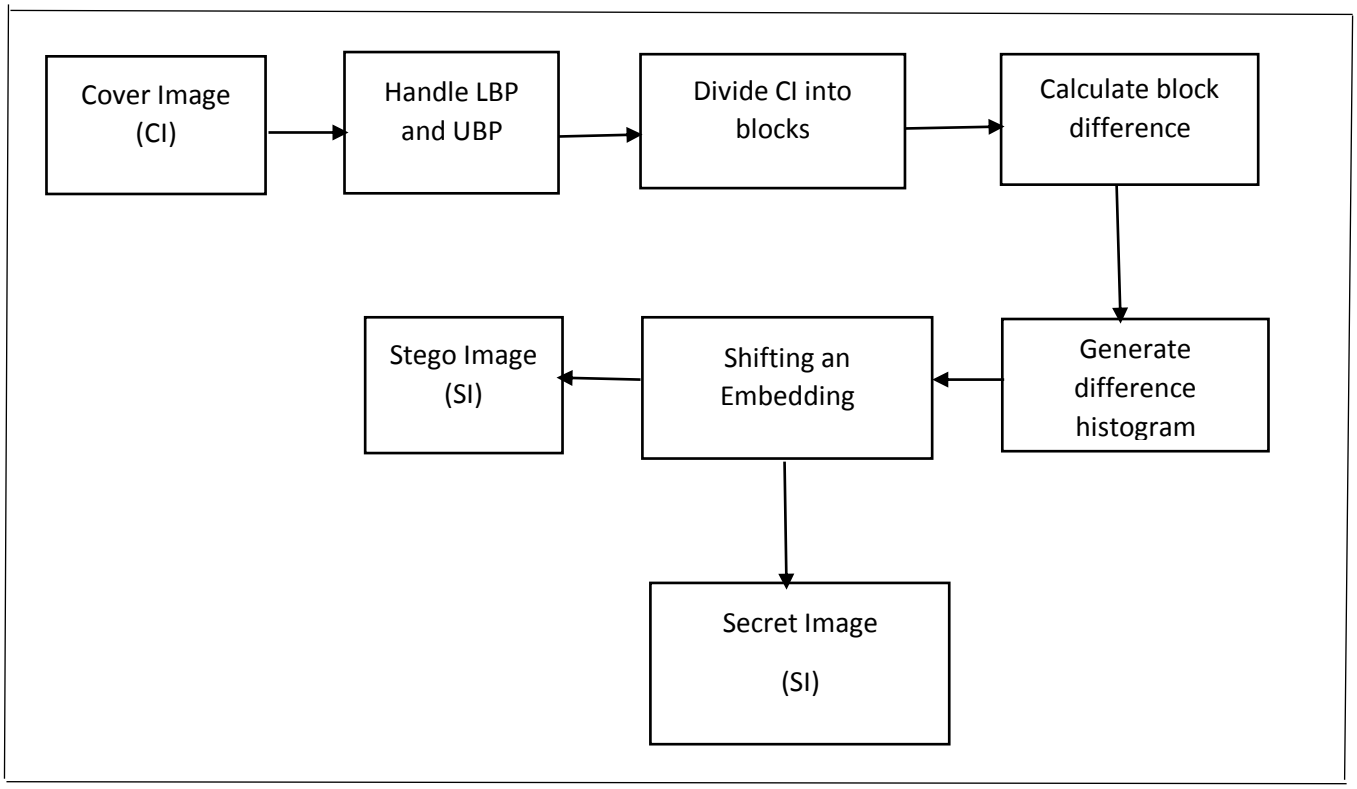

Fig 2: Block Diagram of Embedding Process

The bins are usually specified as consecutive, non-overlapping intervals of a variable. The bins (intervals) must be adjacent, and are often (but are not required to be) of equal size. By generating histogram secret information is embedded by the cover image.

The gray scale image that is to be encrypted is in fig 3 and the cover image using which the image is to be encrypted is in Fig 4. The encrypted secrete image is in Fig 5.

Fig 3: Image to be Encrypted

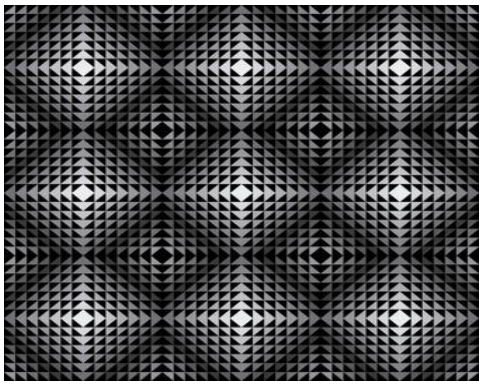

Fig 4: Cover Image

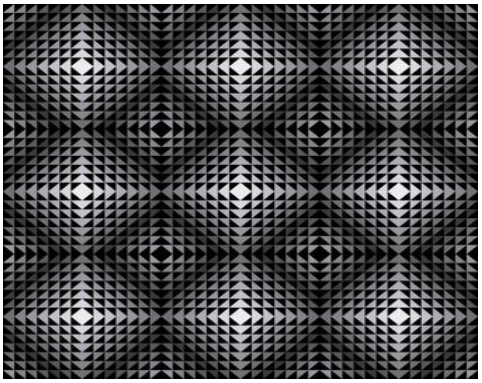

Fig 5: Encrypted Image

C. EXTRACTION PROCESS

The extraction phase is reverse of embedding phase. In the extraction process the stego-image (i.e., the image which is encrypted) is divided into non-overlapping blocks. In every block the reference pixel is chosen as done in the embedding process. Using the block difference in the difference histogram the secret-data is extracted. If the pixel has the difference value p, extracted data bit is 0 and if it is p+1, extracted data bit is 1. The original cover image is also extracted after extracting the secret data and the lower bound pixel and upper bound pixel is also recovered and finally after completing the extraction process the output is the extracted secret image and the cover is original cover-image. MSE (Mean Signal Error) and PSNR (Peak Signal to Noise Ratio) are also calculated in embedding process which is used in the extraction process. And the process takes place as shown in the figure 7.The output of this step is shown in figure 6 that is the original image with no loss of data.

Fig 6: Extracted image

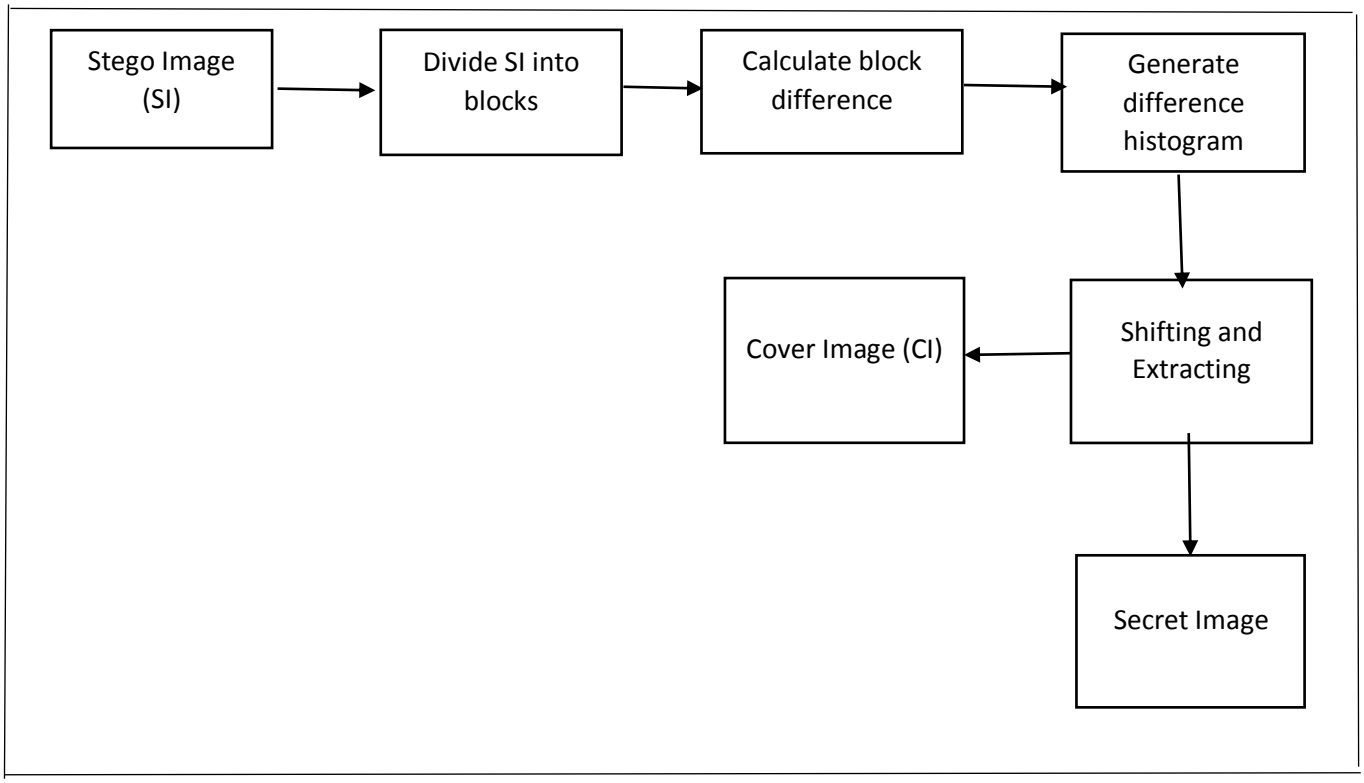

Fig 7: Block Diagram of Extraction Process

V. ALGORITHM

- Determine the difference of neighboring pixel values
- Calculate the variably bits in that difference
- Few differences are decided to be expandable by 1-bit so that builds the variably bits
- Generating a location-map and it consists of location data of all chosen extendable difference-values.
- Collecting unique LSB values
- Embed data by substitution i.e. embed the location-map, original LSBs, and a payload and an inverse integer transform
- Determine the difference of neighboring pixel values
- Determine the alterable bits in that difference

- Collect least significant bits of difference values
- Separate the packed original alterable bit-stream, decode the location-map
- Decompress the compressed separated bit-streams and recreate the original image replacing the alterable bits
- To reconstruct the restored-image apply the inverse integer transform.

VI. CONCLUSION

In this project we will be able to hide the gray scale secret-image efficiently by a cover-image to keep the image secured by the attackers. The main objectives are to design and develop suitable algorithms.

The data embedding is performed after dividing the image into blocks, this helps to distribute the message bits along the whole image and also improves the hiding capacity. And also this technique avoids data loss which is one of the major problem by generating histograms. This work can be extended to color images.

REFERENCES

[1] Al-Shatnawi A. M, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, vol. 6, no. 79, pp. 3907 – 3915, and 2012.

[2] Anderson, R. J. & Petitcolas, F. A. P, "On the limits of steganography", IEEE Journal of selected Areas in Communications, vol. 16, no. 4, pp. 474–481, 1998.

[3] Lincy Rachel Mathews., Arathy C. Haran V, "Histogram Shifting Based Reversible Data Hiding", International journal of Engineering Trends and Technology(IJETT)- vol. 10 Number 10, April 2014.

[4] Cachin C, "An Information-Theoretic Model for Steganography" in Proceedings of the Second International Workshop on Information Hiding, D. Aucsmith, ed. vol. 1525 of Lecture Notes in Computer Science, Berlin, SpringerVerlag, pp. 306–318, 1998.

[5] Chan C. K. and Cheng L. M., "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, pp. 469-474, 2004.

[6] Chandramouli R., Kharrazi M., and Memon N., "Image Steganography and Steganalysis: Concepts and Practice", International Workshop on Digital Watermarking (IWDW), Seoul, pp. 35-49, October 2003.

CONTACT DETAILS

Tejaswini H N (Author)

Final year BE pursuing in Computer Science

Department of Computer Science & Engineering,

Malnad college of Engineering, Hassan

E-Mail: tejasvininagesh200@gmail.com

Chaitra S (Author)

Final year BE pursuing in Computer Science

Department of Computer Science & Engineering,

Malnad college of Engineering, Hassan

E-Mail: Chaitra.chinnu25@gmail.com

Soundarya M (Author)

Final year BE pursuing in Computer Science

Department of Computer Science & Engineering,

Malnad college of Engineering, Hassan

E-Mail: Soundarya.megha12@gmail.com

Monika M M (Author)

Final year BE pursuing in Computer Science

Department of Computer Science & Engineering,

Malnad college of Engineering, Hassan

E-Mail: monikahassan46@gmail.com

Ms. Ayeesha Siddiqha (Co-Author)

B.E, MTech

Assistant Professor,

Malnad College of Engineering, Hassan

E-Mail: ayeeshasidiqha4@gmail.com

Ms. Shruthi T R (Co-Author)

B.E, MTech

Assistant Professor,

Malnad college of Engineering, Hassan

E-Mail: shruthi7129@gmail.com

