

# Advance Scheme for Secret Data Hiding System using Hop-field & LSB

Ishwarjot Singh<sup>1</sup>, J. P. Singh Raina<sup>2</sup>

<sup>1</sup>Research Fellow, <sup>2</sup>Asst. Professor

<sup>1,2</sup>Baba Banda Singh Bahadur Institute of Engg. & Tech., Fatehgarh Sahib, Punjab.

**Abstract** — Security is a major concern where confidential data can be transfer through internet. Steganography is an effective means of hiding data to protect the data from unauthorized or unwanted viewing. In this work, Image can be used to hide confidential data. We use hop field algorithm & LSB technique in this work. Firstly Hop-field algorithm is used on the original image and it gives optimized results then key can be generating from these results using LSB technique. A secret data can be hide behind of this resulting image and it forms a stego image. All the data can be hide in the stego-image. This increases security means protecting our confidential information from unauthorized access. On the receiver side all the process work in inverse order and extract the hidden data from the image.

**Keywords**— Security, Data hiding, Steganography, Hop-field, LSB.

## I. INTRODUCTION

Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually un-encrypt the data. A solution to this problem is steganography. The ancient art of hiding messages so that they are not detectable. No substitution or permutation was used. The hidden message is plain, but unsuspecting to the reader. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood.

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret.

Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “*stegos*” meaning “cover” and “*grafia*” meaning “writing” [1] defining it as “covered writing”. In image steganography the information is hidden exclusively in images. The idea and practice of hiding information has a long history. In *Histories* the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message [2]. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [3]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide. For example, the picture of our cat could conceal the plans for our company's latest technical innovation.

### 1.1 Uses of Steganography

1. Steganography can be a solution which makes it possible to send news and information without being

censored and without the fear of the messages being intercepted and traced back to us.

2. It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside.

3. Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, Steganographic methods can be used to hide this.

4. E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open ecommerce transaction verification.

5. Paired with existing communication methods, steganography can be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital steganography provides vast potential for both types. Businesses may have similar concerns Regarding trade secrets or new product information.

6. The transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites.

## II. STEGANOGRAPHY & SECURITY

Steganography is an effective means of hiding data, thereby protecting the data from unauthorized or unwanted viewing. But stego is simply one of many ways to protect the confidentiality of data. It is probably best used in conjunction with another data-hiding method. When used in combination, these methods can all be a part of a layered security approach. Some good complementary methods include:

### A. Encryption

Encryption is the process of passing data or plaintext through a series of mathematical operations that generate an alternate form of the original data known as ciphertext. The encrypted data can only be read by parties who have been given the necessary key to decrypt the ciphertext back into its original plaintext form. Encryption doesn't hide data, but it does make it hard to read!

### B. Hidden directories (Windows)

Windows offers this feature, which allows users to hide files. Using this feature is as easy as changing the properties of a directory to "hidden", and hoping that no one displays all types of files in their explorer.

Hiding directories (Unix) in existing directories that have a lot of files, such as in the /dev directory on a Unix implementation, or making a directory that starts with three dots (...) versus the normal single or double dot.

### C. Covert channels

Some tools can be used to transmit valuable data in seemingly normal network traffic. One such tool is Loki. Loki is a tool that hides data in ICMP traffic (like ping).

## 2.1 Confidential Communication and Secret Data Storing

The "secrecy" of the embedded data is essential in this area [16]. Historically, steganography have been approached in this area. Steganography provides us with:

- Potential capability to hide the existence of confidential data
- Hardness of detecting the hidden (i.e., embedded) data
- Strengthening of the secrecy of the encrypted data

In practice, when you use some steganography, you must first select a vessel data according to the size of the embedding data. The vessel should be innocuous. Then, you embed the confidential data by using an embedding program (which is one component of the

steganography software) together with some key. When extracting, you (or your party) use an extracting program (another component) to recover the embedded data by the same key ("common key" in terms of cryptography). In this case you need a "key negotiation" before you start communication.

Attaching a stego file to an e-mail message is the simplest example in this application area. But you and your party must do a "sending-and-receiving" action that could be noticed by a third party. So, e-mailing is not a completely secret communication method. There is an easy method that has no key-negotiation. We have a model of "Anonymous Covert Mailing System." There is some other communication method that uses the Internet Webpage. In this method you don't need to send anything to your party, and no one can detect your communication.

Each secrecy based application needs an embedding process which leaves the smallest embedding evidence. You may follow the following:

- Choose a large vessel, larger the better, compared with the embedding data.
- Discard the original vessel after embedding.

For example, in the case of Qtech, Hide & View, it leaves some latent embedding evidence even if the vessel has a very large embedding capacity. You are recommended to embed only 25% or less (for PNG / BMP output) of the maximum capacity, or only 3% of the vessel size (for JPEG output).

## **2.2 Protection of Data Alteration**

We take advantage of the fragility of the embedded data in this application area [12]. If it is implemented, people can send their "digital certificate data" to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

## **2.3 Access Control System for Digital Content Distribution**

Since the advent of cybernetics, the field of communication has been revolutionized. We can rightly call 21<sup>st</sup> century the era of computers, internet and information technology. The internet as with all path breaking technological developments gives us every opportunity to act as global community; advertise and operate across all frontiers, over borders and beyond the control of any national Government. The intense volume of information, the simplicity of its transfer and transparency in this field create a lot of problems. Ownership of information is hard to protect; the illicit reuse of copyright material

is commonplace in our times. Corporate houses all over the world have the apprehension of their data being misused by their competitors with ulterior motive. Even the Governments have grown highly cautious and alert in this regard. Hence the experts in the field of cybernetics urged by the principle or maxim: 'necessity is the mother of all inventions' developed steganography for the purpose of keeping the important data and information secret. Several international institutions are also striving to produce data protection principles which may be recognised and adhered to internationally. Confidential information and data are of a great significance in the modern world of globalization dominated by competition. A trader or commercial entity seeks to obtain as much information as possible concerning the business of his rivals and to keep its own information and data as concealed as possible. The information may be a trade secret, for example, a method of production not protected by a patent, or a business secret, such as financial structuring of a big house or a piece of domestic 'in house' information like the salary scales of employees, or the efficiency of the firm's data collection and conservation.

## **III. PROPOSED SCHEME FOR DATA HIDING**

Image steganography basically deals with hiding the data in the digital representation of the image. So, this work proposed enhanced approach using Hop-field & LSB techniques.

### **3.1 Proposed Model**

The proposed modal focuses on following objectives which are helpful in increasing security to prevent from unauthorized access and are implemented using MATLAB.

- a. To propose Enhanced Data Hiding Scheme using Hop-field & LSB Encoding Schemes.
- b. To implement security using LSB key generation scheme.
- c. Prevent from unauthorized access on confidential data.

In this proposed work, Hop-field algorithm is firstly used to give an optimized result and key generation can be done by using LSB algorithm. After Key generation, a secret data can be embedded to original image & it forms a stego-image which hides our secret data.

### **3.2 Basic Block Design**

As data transmission using internet increases with time. So, security is the major need to prevent our data from unauthorized access. This proposed enhanced scheme use Hop-field & LSB Encoding schemes & generate a stego-image where data can be hide.

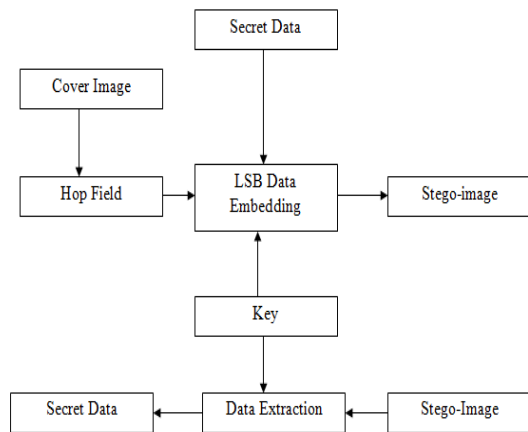


Fig 1: Basic Block Design of Proposed Work

This scheme is proposed to enhance the security & data hiding using steganography. The Block design of the proposed work is shown in Fig 1.

**3.3 Algorithm level Design**

This work can be divided into two parts:

- 1) Secret Data Hiding
- 2) Secret Data Retrieving

Fig 2(a) & 2(b) represents the algorithm level design of the proposed system for both process that is hiding & retrieving.

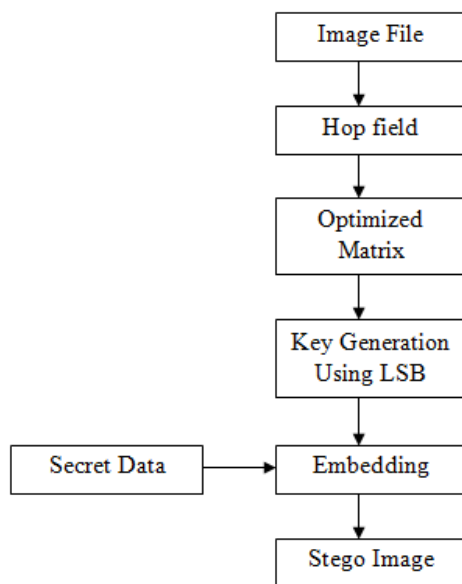


Fig 2(a): Secret Data Hiding

In the secret data hiding process, firstly hop filed algorithm is applied on the cover image file which results as an optimized value. Then key generation process can be done using LSB technique. Now secret data can be embedded to it & it results as a

stego-image. The whole process can be shown in fig 2(a) and it hides the data behind the cover image.

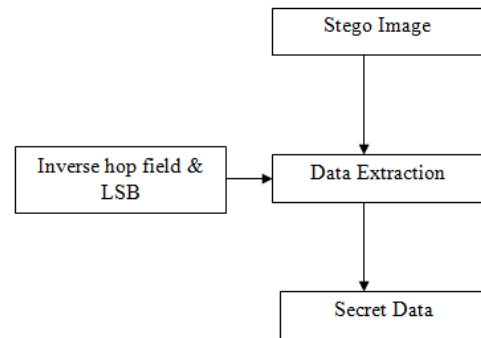






Fig 2(b): Secret Data Retrieving

In the secret data retrieving process, stego-image is used to extract the secret data by applying inverse of the hop field & LSB. The whole process can be shown in fig 2(b) and it results as a extraction of the secret data.

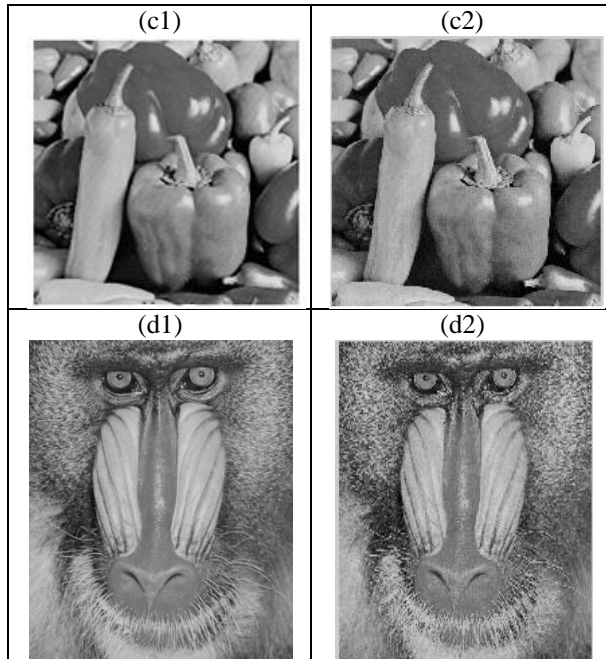
**IV. RESULTS AND ANALYSIS**

The requirements of a secret data hiding system when used for stegnographic purposes are of high hiding capacity and imperceptibility. Keeping in view some conflicting features a reasonable amount of data has been taken to be embedded in the cover medium so as to keep degradation in the image quality minimum. For the testing the efficiency of the proposed scheme a set of four standard grey scale test images were used. Table 1 shows all the used cover images with their corresponding stego-image.

Table 1: Cover Images & their stego images

Cover Image	Stego Image
(a1) 	(a2) 
(b1) 	(b2) 





(c)	37.65	40.36
(d)	37.64	40.89

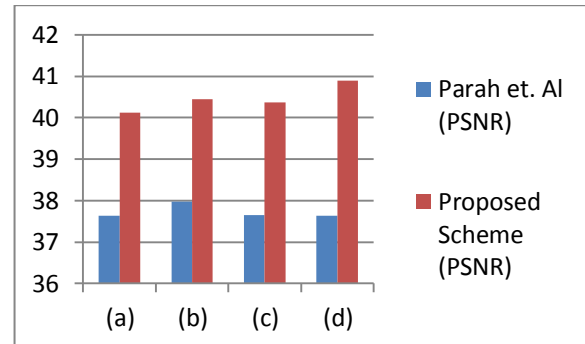


Fig 3: Previous Approach & Enhanced Approach

Table 2 presents details of cover images with corresponding peak signal to noise ratio PSNR. Further a comparison of the proposed secret data hiding scheme with that of Parah et. al [17] can be seen in table 2. Figure 3 graphical comparisons between the proposed technique and that of Parah et. al. The PSNR has been calculated as follows.

**Peak Signal to Noise Ratio (PSNR):**

It is an important image, objective, quality index. It is actually a measure of quality of image when external data is embedded in it. It gives an idea about how much deterioration has embedding caused to the image. It is represented as

$$PSNR = 10 \log_{10} \frac{255^2}{mse} \text{ db}$$

Where ‘mse’ is mean square error and is given by

$$mse = \left[ \frac{1}{N * M} \right]^2 \sum_{i=1}^N \sum_{j=1}^N (X_{ij} - \bar{X}_{ij})^2$$

Where N and M are image dimensions, and represent original and stego images respectively.

Table 2: PSNR of Proposed scheme & Previous

Cover Image	Previous Technique	Proposed Scheme
(a)	37.63	40.12
(b)	37.97	40.45

**V. CONCLUSION**

In this paper, we proposed a secret data hiding approach, which is Enhanced Hiding Approach using Hop-field & LSB techniques, for securing confidential data from unauthorized access. Hop-field helps to make data optimized & LSB generates a key. Embedding is done using this technique helps to least deterioration in the original image. This enhanced approach can achieve better results than the previous approach which used blind detection technique.

**REFERENCES**

- [1] Khosravi Sara, Abbasi Dezfoli Mashallah, Yektaie Mohammad Hossein, et al, *A new steganography method based on hiop (higher intensity of pixel) algorithm and strassen's matrix multiplication*, Journal of Global Research in Computer Science Volume 2, No. 1, January 2011.
- [2] R.Amirtharajan, Adharsh.D, Vignesh.V, R.John Bosco Balaguru, et al, *PVD blend with pixel indicator - OPAP composite for high fidelity steganography*, International Journal of Computer Applications Volume 7– No.9, (0975 – 8887) October 2010.
- [3] Namita Tiwari, Madhu Shandilya, et al, *Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth*, International Journal of Security and Its Applications Vol. 4, No. 4, October, 2010.
- [4] Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaq K and John Bosco Balaguru Rayappan, R.Amirtharajan, et al, *Colour Guided Colour Image Steganography*, Universal Journal of Computer Science and Engineering Technology 1 (1), 16-23, Oct. 2010. © 2010 UniCSE, ISSN: 2219-2158.
- [5] Abdul-Rahman Shaheen, Mahmoud Ankeer, Muhammed Abu Ghalioun, et al, *Using Pixel Indicator Technique in Images for Better Steganography*, Journal Of Emerging Technologies In Web Intelligence, Vol. 2, No.1, February 2010.
- [6] Ali Akbar Nikoukar, et al, *An Image Steganography*

- Method with High Hiding Capacity Based on RGB Image*, International Journal of Signal and Image Processing Nikoukar / An Image Steganography Method with High Hiding Capacity / Vol.1/Iss.4 pp. 238-241, 2010.
- [7] Hussain, M. Hussain, M, et al, *Pixel intensity based high capacity data embedding method*, Information and Emerging Technologies (ICIET), 2010 International Conference, on page(s): 1 – 5, June 2010.
- [8] Adnan Abdul-Aziz Gutub, et al, *Pixel Indicator Technique for RGB Image Steganography*, Journal Of Emerging Technologies In Web Intelligence, Vol. 2, No.1, February 2010.
- [9] Piyush Marwaha, Paresh Marwaha, et al, *Visual cryptographic steganography in images*, 2010 Second International conference on Computing, Communication and Networking Technologies, 2010.
- [10] Gutub A., Al-Qahtani A., Tabakh A., et al, *Triple-A: Secure RGB image steganography based on randomization*, Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS, on page(s): 400 – 403, May 2009.
- [11] Parvez, M.T., Gutub, A.A.-A., et al, *RGB Intensity Based Variable-Bits Image Steganography*, Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE, on page(s): 1322 – 1327, Dec. 2008.
- [12] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi, et al, *Pixel Indicator High Capacity Technique For RGB Image Based steganography*, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E. March 2008.
- [13] Mohammad Tanvir Parvez and Adnan Abdul-Aziz Gutub, et al, *RGB Intensity Based Variable-Bits Image Steganography*, 2008 IEEE Asia-Pacific Services Computing Conference.
- [14] Bailey K., Curran K., et al, *An evaluation of image based steganography methods*, Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, July 2006.
- [15] Eiji Kawaguchi, et al, *A Model of Anonymous Covert Mailing System Using Steganographic Scheme*, in information modelling and knowledge bases xiv, H. Yaakkola et al (Eds), IOS Press, pp.81-85, 2003.
- [16] Eiji Kawaguchi, Michiro Maeta, Hideki Noda and Koichi Nozaki, et al, *A Model of Digital Contents Access Control System Using Steganographic Information Hiding Scheme*, Information Modelling and Knowledge Bases IX, pp.255-265, 1998.
- [17] Shabir A. Parah, Javaid A. Sheikh, & G.M. Bhat, “Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique” International Conference on Emerging Trends in Science, Engineering and Technology-2012.