# New Encrypted Steganography Approach

**Saba Mohammed Husain**
*Information technology college-Babylon university*
Saba_muh@ymail.com

## Abstract

The proposed research Provides an approach for hiding an encrypted text in side a digital image. Where the text is encrypted in a complex manner used method of PlayFair to encrypt clear text and to increase security put lettering ciphertext on the geometric shape clockwise and then we write the ciphertext output in the form of lines, taken new ciphertext and converted to Ascii code and then to binary and hidden text in bits least importance in the picture. The results were good by PNSR scale.

**Keywords**: security, cryptography.

## الخلاصة

يوفر البحث المقترح طريقة لتشفير النص واخفائه داخل صورة رقمية، حيث يتم تشفير النص بطريقة معقدة تستخدم طريقة Playfair لتشفير النص الواضح ولزيادة الامنية نضع حروف النص المشفر على شكل هندسي باتجاه عقارب الساعة وبعد ذلك نكتب النص المشفر الناتج على شكل اسطر ، يؤخذ النص المشفر الجديد ويحول الى Ascii code وبعدها الى binary ويخفى النص في البتات الاقل اهمية في الصورة. وكانت النتائج جيدة حسب مقياس PNSR.

**الكلمات المفتاحية:** الامنية، تشفير .

## 1. Introduction

With the development of PC system, security of information has turned into a noteworthy concern and hence information concealing procedure has pulled in individuals around the world. Steganography methods are utilized to address computerized copyrights administration, ensure data, and hide privileged insights. Information concealing strategies give an intriguing test to advanced scientific agents. Information becomes an integral part for computer security that need to be secured against unauthorized access. Hence, the information concealing field comes to hide a sequence of bits in a cover media. The cover media consists of many mediums such as video, image, audio and texts.

Computerized data represent in term of machine bits in computer systems. There are three criteria in information security to manipulate the data in computer. The three criteria's are CIA (Congenitally, integrity and availability). Steganography and cryptography are two methods of information hiding. These methods provide good tools to secure the data and provide the security criteria's. in these two methods, we can hide message in text, audio, video and others medium.

Steganography can be defined as a science of hide the existence object in invisible/ visible The main objective of steganography is to not attract the attacker or eavesdropping to detect this message and then analysis the secured embedded message. The secured message in steganography should be robustness against detectability, rotating and compression (Shamim Ahmed Laskar,2012)

Implementation of steganography may include errors and noise. There are two types of steganography methods visible and invisible. The visible method not concealing the data inside the cover, while the invisible method conceal the data inside the cover medium.

System security is imperative at the present time as the quantity of information traded developments on the web. Consequently, the security and dependability of the information that needs to ensure close to unapproved get to and utilization. This is making it increasingly in the field of hiding information. In addition, the broadcast technology and the rapid deployment also requires an alternative solution to hide the information. In another direction, steganography is fundamentally concealing the message so that the analyzer (attacker) can't see the steganogram. Steganography provides a robust way to hide a secret steganogram in Picture, Video, and Audio files. For the human perception, pictures is more convenient with Human Visual system (HVS). (Provos, 2001).

Steganography intimates information or a record that has been hidden inside an electronic Picture, Video or Audio file. Pictures can be more than what we see with our Human Visual System (HVS); along these lines, they can go on more than just 1000 words, (Vijaykumar Sharma, 2012).

Many researches adopt different methods for steganography. adopt method to hide the secret message based on identifying the identical bits between the object message and cover medium. In this method, The LSB method is compared with the proposed method. (Al-Shatnawi, 2012)

According to (Sudha (2012), the LSB method is proposed to hide the secret message in a text using insertion method with Chaos. The proposed system is evaluated using the Signal to noise ratio (PSNR) and mean square error (MSE) on a cover intensity image.

## 2. Overview of Steganography

The Steganography term is derived from Greek source and it is divided into two main steps. The "Steganos" which means secret or cover and graphic" which means "writing" or text. (Al-Shatnawi, 2012)

The inspiration driving creats picture Steganography systems as indicated by its utilization in different associations to impart between its individuals, and in addition, it can be utilized for correspondence between individuals from the military or insight agents or operators of organizations to shroud mystery messages or in the field of undercover work. The primary objective of utilizing the Steganography is to abstain from attracting gattention to the transmission of shrouded data. In the event that distrust is raised, then this objective that has been required to accomplish the security of the mystery messages, in light of the fact that if the programmers notices any adjustment in the sent message then this onlooker will attempt to know the concealed data inside the message,( Wu & Wang, 2010, Corporation, 2005).

Many methods are used to embed the steganogram inside the cover object. Embedding the watermark and steganography methods are used in same manner and in the some cases leads to treat equally. These methods comes to play a major role in the art of steganography and to avoid suspicion that leads to discover the hidden message. Some methods of steganography is used to reduce the visible detection of the secret message. In another direction, the hiding secret message in the carrier may cause a degradation in the carrier due to the change in some properties. The human eyes may check this degradation and can extract the hidden message using tools of analysis (Johnson2003).

In this paper, we propose a steganography method which hide the text inside the image. The characters of the plain text are encrypted using play-fair method and then we insert the encrypted text in the cover image. In general, the steganography model is shown in figure (1)
(Shikha Sharda1, Sumit Budhiraja2,2013)

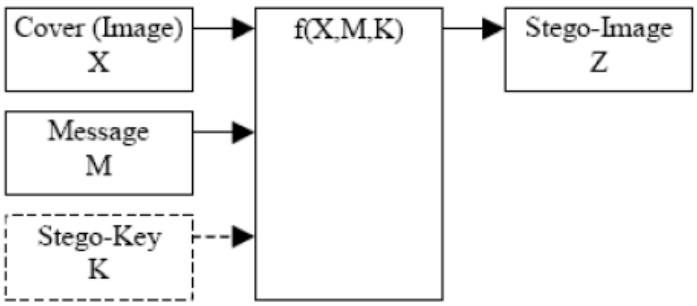


**Figure 1: general model of Steganography Encoder**

Where X is the cover image to include the secret message (M) . The play-fair method is used stego-key (K) to generate the f(X,Y,K). the stego-image (z) is then used to generate the proposed system in this paper.

**2.1 Stenographic Techniques**

There are a lot of systems in organizing stenographic techniques. These philosophies can be described according to the kind of spreads used with riddle correspondences. Another credibility is finished by method for sorting such approachs depending upon the kind of spread change authoritatively associated amid the time spent embedding. The second approach is grasped in this work ,yet now and again a watchful request is unreasonable, (Kruus2003).

**2.2 Stream generators**

direct feedback development registers are extensively used as a piece of key stream generators in light of the way that they are suitable for gear execution, and they create progressions having far reaching periods and incredible quantifiable properties, and are immediately explored using logarithmic frameworks.

For essentially all possible secret keys, the yield gathering of a LFSR-based key stream generator should have the going with properties:

1. broad period.
2. broad straight multifaceted nature.
3. extraordinary quantifiable properties .

It is underlined that these properties are simply major conditions for a key stream generator to be considered cryptographically secure. Since numerical affirmations of security of such generators are not known, such generators must be considered computationally secure.

**2.3. Play fair**

The method encrypts sets of letters, rather than single letters as in the straightforward substitution figure. The Playfair is fundamentally harder to break subsequent to the recurrence examination utilized for basic substitution figures does not work with it. Recurrence examination can even now be embraced, however on the 25*25=625 conceivable digraphs as opposed to the 25 conceivable monographs.

The Playfair figure utilizes a 5 by 5 table containing a catch phrase or expression. Emorization of the catchphrase and 4 straightforward tenets was all that required to make the 5 by 5 table and utilize the figure to make the key table as shown in table (1), one would first fill in the spaces in the table with the letters of the watchword (dropping any duplicate letters), then fill the remaining spaces with the straggling leftovers of the letters of the letters all together all together (for the most part blocking "Q" to diminish the letters keeping in mind the end goal to fit; distinctive adjustments put both "I" and "J" in the same space). The key can be formed in the top segments of the table, from left to right, or in some other illustration. For instance, a twisting beginning in the upper-left-hand corner and fulfillment in within. The watchword together with the conventions for filling in the 5 by 5 table constitute the figure key. (Avi Kak,2016)

Table (1): Play-fair alphabetic matrix

| | | | | |
|---|---|---|---|---|
| A | B | C | D | E |
| F | G | H | I,J | K |
| L | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

## 3. Proposed Technique Steps

System receives a secret message ( clear text ) and encrypts the text in a play-fair method and then represent letters resulting from encryption geometrically clockwise with predefined dimensions shape, then turn the output format to a line of characters which converted the ASCII code of each character and turn it into binary form, which hiding in LSB manner.

**3.1. The steps of the play-fair:-**

One parts the content into sets of letters (bigrams) and apply the accompanying guidelines as indicated by the letters positions in the grid :

1-if the 2 letters are indistinguishable put another letter (for instance X or Q) after the main letter and figure the new bigram subsequently framed

2-if the two letters are on the same line, supplant them by the ones to their right side (loop to one side if the edge of the framework is reached),

3-if the 2 letters are on the same section, supplant them by the ones simply under (loop to the top if the base of the framework is reached),

4-else, supplant the letters by the ones shaping a rectangle with the first pair. The figured bigram starts with the letter on the same line as the first letter to figure

- **Put the cipher text as geometric form with clockwise.**
- **Then write the cipher text result as form line.**
- **Convert the new cipher text into ASCI code then to binary after that hide the data in LST bit.**
-

**3.2. Encryption process for suggested system:**

1- Divide the plain text in to pairs of character.
2- Put the cipher text as geometric form with clockwise direction.
3- Write the cipher text as line form.
4- Convert the new cipher text to Ascii code then to binary after that hide data in LSB in an image.

**Take an example:**

Let have the plain text **((send help soon))**

1- Cut the plain text to Pairs

Se nd he lp so on

2- After using play fair method , get that:-

Se nd he lp so on
Cu co ck mq nt po

3- For increasing the security, put the cipher text as a geometric form with clockwise as shown in table (2):

**Table 2:** clockwise geometric form

| | | |
|---|---|---|
| C | U | C |
| T | P | O |
| N | O | C |
| Q | M | K |

4- Write the cipher text as line form:-

**cuctponocqmk**

5- Then convert the new cipher text to Ascii code as:

**cuctponocqmk**

99117991161121111011199113109107

6-then to a Binary as;-

110 0011111 0101110 0011……..

after that hide data in LFST Bit in an Image.

**3.3. Decryption process:-**

1- Return the ASCII code for each character from the binary number.

2- Recovery the cipher text as one line form

cu ct po no cq mk

3- Put the line latters in a geometric form as clock wise with know the dimension form(above example with 3*4 dimension).

cuc
tpo
noc
qmk

4-put the latters as line form

cucockmqntpo then

5- Application decoder play fair for each latter.

Sendhelpsoon

The proposed system is described in figure (2) below

## 4. Performance Measure using Peak Signal to Noise Ratio (PSNR)

The proposed method is evaluated using the performance PSNR and Mean Square Error (MSE) . The value of PSNR is measured the degree of degradation of steganography method, where the higher value represent the more quality in the stego image, while the low value makes the stego image in low quality. In the event that the spread picture is C of size M × M and the stego picture is S of size N × N, then every spread picture C and stego picture S will have pixel (x, y) from 0 to M-1 and 0 to N-1 independentl, the PSNR is then c:

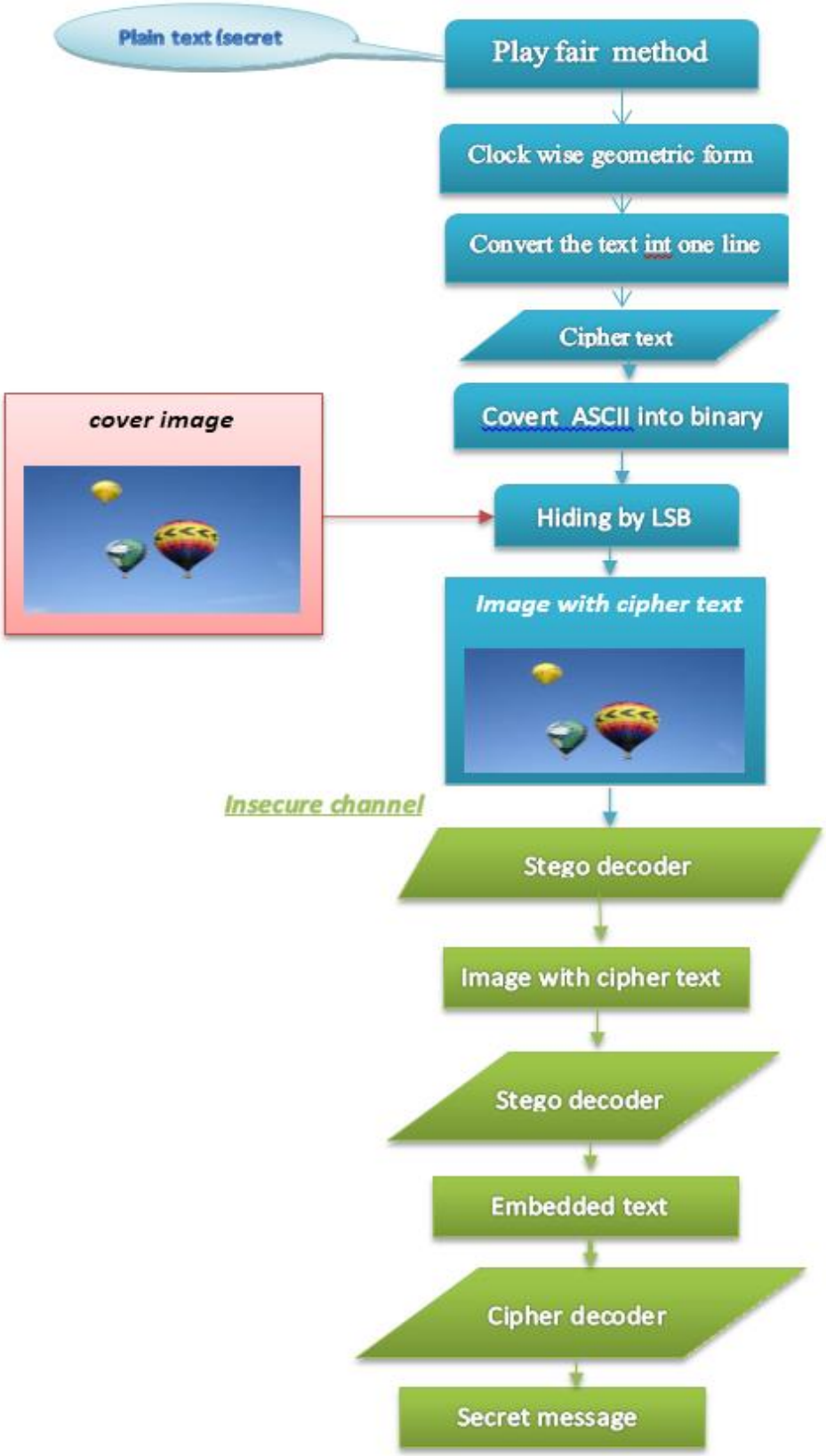


**Figure 2: The Steganography proposes system**

## 5. Experimental Results

Table (2) show the experimental result of the hiding cipher text size in cover image and the PSNR in several images.

**Table 2: PSNR values using the proposed system**

| Image name | Plan text size | PSNR |
|---|---|---|
| I1 | 10 KB | 83.3050 |
| I2 | 18KB | 81.0261 |
| I3 | 20KB | 79.5071 |
| I4 | 30KB | 51.9897 |

Figures (3) ,(4), (5) and (6) show the original image with its histogram.

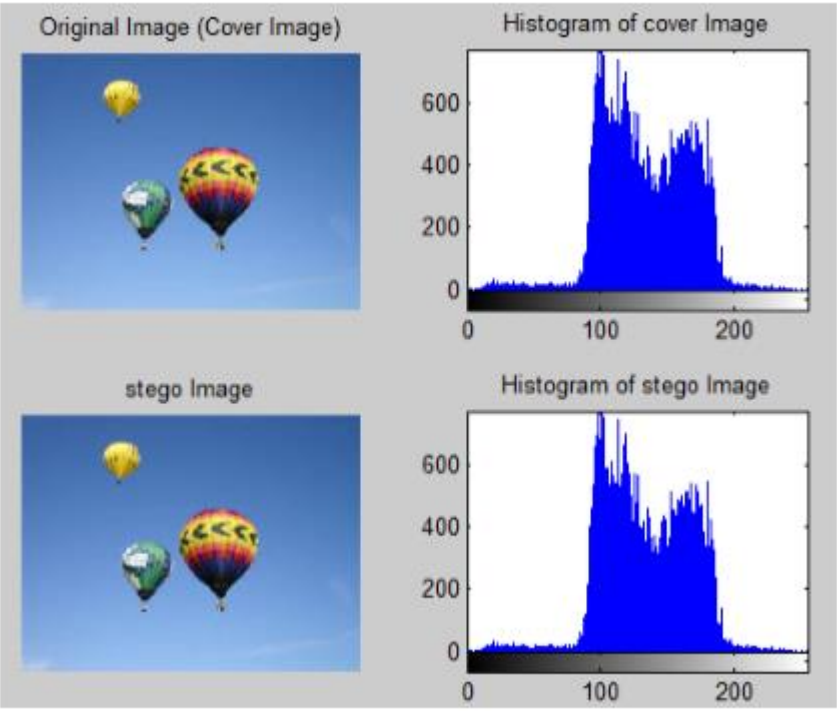


**Figure 3:** Histogram of cover image-1

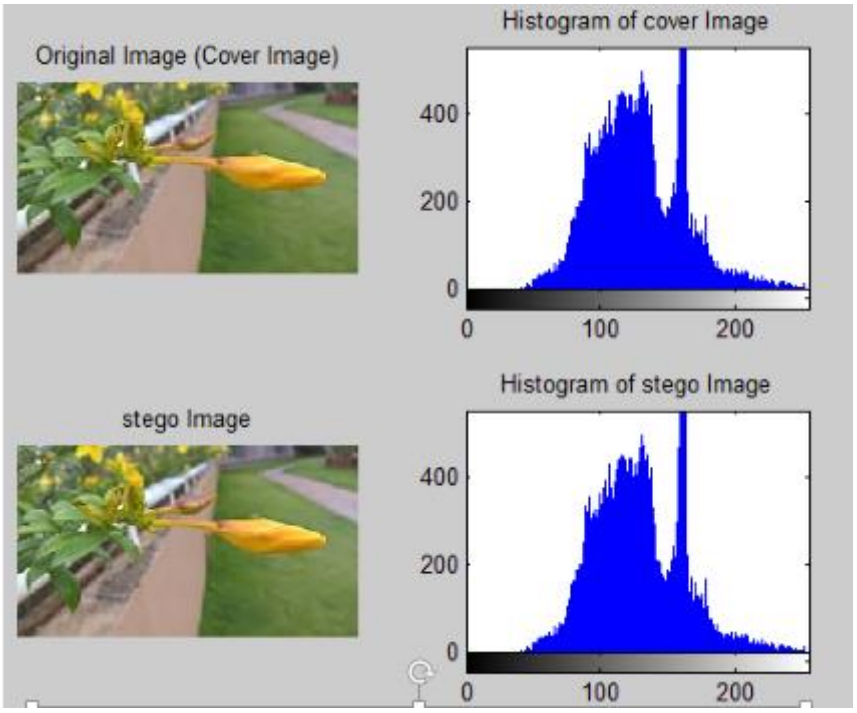


**Figure 4:** Histogram of other cover image-**2**

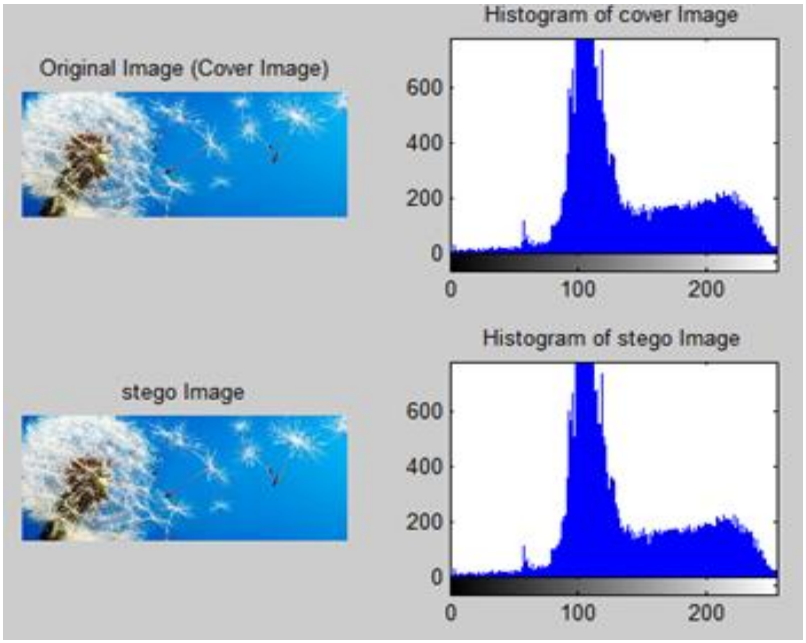


**Figure 5:** Histogram of other cover image-3

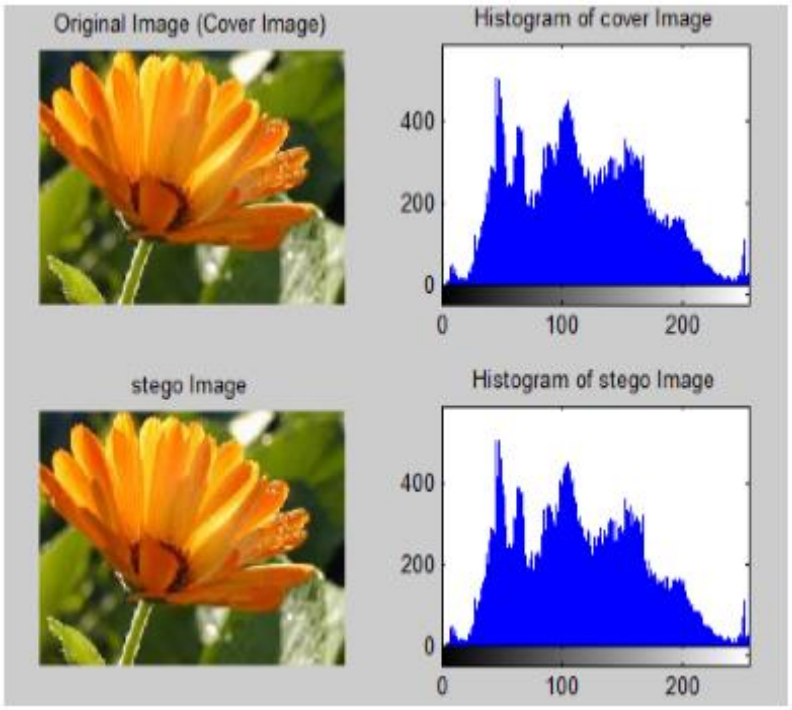


**Figure 6:** Histogram of other cover image-4

## 6. Conclusion

Use a hybrid method for text encrypted is the purpose of the increasing information security force. Also, scattered text by using geometric shape clockwise after using playfaire cypher method. Increasing the length of the text leads to increased complexity of the method. Also, hide text within a digital image give a second layer of security force. Then there are three level of security to the secure message.

## References

Bhavana.S1 and K.L.Sudha2 "TEXT STEGANOGRAPHY USING LSB INSERTION METHOD ALONG WITH CHAOS THEORY', nternational Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.2, April 2012.

Atallah M. Al-Shatnawi, 2012,"A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915.

Kruus, P.; C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal. [On line], 5(1), pp. 41-52. Available: http://www.isso.sparta.com/documents/asrjv5.pdf#page=47 [Oct., 2011].

Vijaykumar Sharma , Vishal Shrivastava, 15th February 2012, A STEGANOGRAPHY ALGORITHM FOR HIDING IMAGE IN IMAGE BY IMPROVED LSB SUBSTITUTION BY MINIMIZE DETECTION, Journal of Theoretical and Applied Information Technology, Vol. 36 No.1 © 2005 - 2012 JATIT & LLS. All rights reserved.

Shamim Ahmed Laskar, December 2012 "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems ( IJDMS ) Vol.4, No.6.

Shikha Sharda1, Sumit Budhiraja2, 2013" Image Steganography: A Review", nternational Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013).

Avi Kak (kak@purdue.edu , January 15, 2016, "Computer and Network Security". Provos, N. January 31, 2001,"Probabilistic Methods for Improving Information Hiding", *CITI Technical Report 01-1*.