*International Journal on Emerging Technologies* **3**(1): 48-54(2012) **ISSN No. (Print) : 0975-8364**
**ISSN No. (Online) : 2249-3255**

# Techniques of Steganography for Securing Information: A Survey

***Sanjay Bajpai* and Dr. Kanak Saxena*****

**Department of Computer Applications, Lakshmi Narain College of Technology, Bhopal, (MP), India*

***Department of Computer Applications, Samrat Ashok Technological Institute, Vidisha, (MP), India*

*(Recieved 23 March 2012 Accepted 15 April 2012)*

**ABSTRACT : The main objective of writing this paper is to explore, as many as possible, algorithms and techniques that have been used by many researchers to provide security to the information using steganography. Steganography is the science that deals with communicating secret data by using any of the multimedia carrier, such as digital image, audio and video files. Cryptography is also used for securing the secret message but in this, feature is visible though it is not readable so point of attack is evident. So, primary goal is to hide the very existence of the embedded data. Features like undetectability, embedding capacity, robustness (resistance to various image processing methods and compression) etc make it different from other related techniques such as water marking and cryptography. This paper provides the summary of various algorithms, analysis with their pros and cons and future scope of the work.**

**Keywords:** Steganography, Digital water marking, Robustness, Compression, Cryptography.

## I. INTRODUCTION

Let us start with the cryptography which is a science for dismantling the meaningful and important information so that any person, whom we do not wish, cannot read it. Many different methods have been developed to encrypt and decrypt data for securing the secrecy of communication. This method gives the clue that some important information is being communicated but not in a readable form. This arouses the curiosity of malicious people who desire to recover or destroy. So the concept of Steganography came into existence.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of communicated information in other media. For example, a secret message hidden in a digital image. The standard and concept of "What You See Is What You Get (WYSIWYG)" which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a steganographer as it does not always hold true. Images can be more than what we see with our Human Visual System (HVS) [1]. Watermarking and finger printing are other two techniques that are closely related to steganography [2]. In the watermarking methods, all the objects are marked in the same way just as to provide a signature to signify the origin or ownership for the purpose of copyright protection [3]. On the other hand, finger printing embeds the unique marks on the distinct copies of the object to protect the licensing agreement. Three techniques are interlinked, steganography, watermarking and cryptography. Their relations are illustrated in Fig. 1 and Table 1 [1].

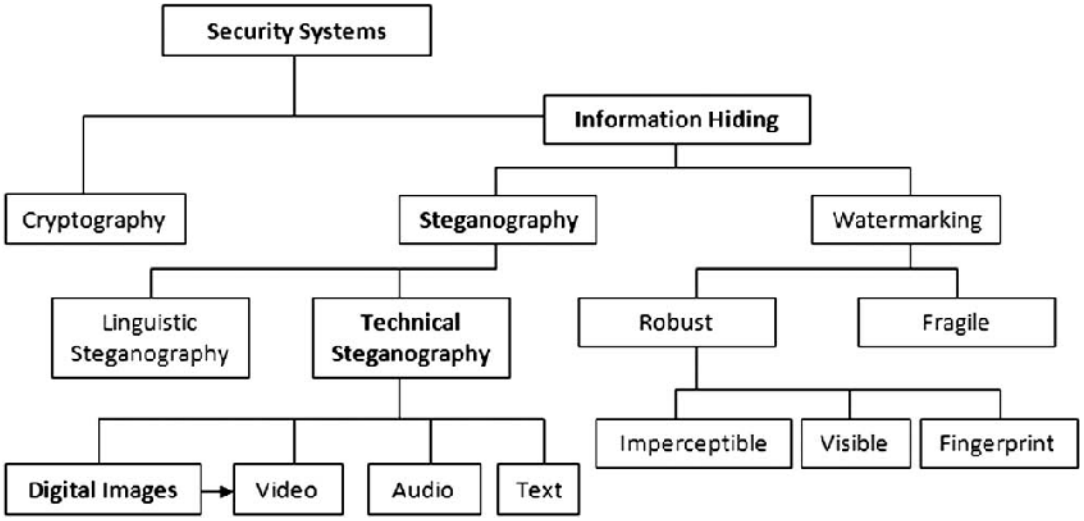


Fig. 1. Different embodiment disciplines of information hiding.

The remainder of this paper is organized as follows. Section 2 briefly discusses the applications of steganography. A few examples and methods used in ancient times to hide a message are described in section 3. Basic mechanisms of hiding secret messages in digital images by manipulating the pixels are described in section 4. Section 5 gives the brief analysis of methods used by various scholars and some comments on the effectiveness. This part also describes their embedding process in brief and draws the attention towards improvements. Finally, the conclusions are presented in section 6.

**Table 1: Comparism of steganography, watermarking and encryption.**

| Criterion/ Method | Steganography | Watermarking | Encryption |
|---|---|---|---|
| Carrier | Any digital media | Mostly image/audio files | Usually text based, with some extensions to image files |
| Secret data | Payload | Watermark | Plain text |
| Key | Optional | | Necessary |
| Detection | Blind | Usually informative | Blind |
| Authentication | Full retrieval of data | Usually achieved by cross correlation | Full retrieval of data |
| Objective | Secret communication | Copyright preserving | Data Protection |
| Result | Stego-file | Watermarked-file | Cipher text |
| Visibility | Never | Sometimes | Always |
| Fails when | It is detected | It is removed/replaced | De-ciphered |

## II. APPLICATIONS OF STEGANOGRAPHY

It is useful in various fields such as confidential communication and secret data storing, protection of data alteration, access control system for digital content distribution, media database systems etc. Other applications are audio-video synchronization, companies' safe circulation of secret data, TCP/IP packets (for instance a unique ID can be embedded into an image to analyze the network traffic of particular users) [4]. Peticolas [5] also discussed about its applications in Medical Imaging System where a privacy is considered necessary between patients' image data and their captions, for e.g., physician's name, patient's name, about the disease and other particulars. Thus, embedding the patients' information in the image could be a useful safety measure.

Abbas Cheddad *et al* [1] discussed about the Japanese firm Fujitsu, that is developing technology to encode data into a printed picture that is invisible to the human eye (data), but can be decoded by a mobile phone with a camera as exemplified in Fig. 2(a) and shown in action in Fig. 2(b). The process takes less than one second as the embedded data is merely 12 bytes. Hence, users will be able to use their cellular phones to capture encoded data.

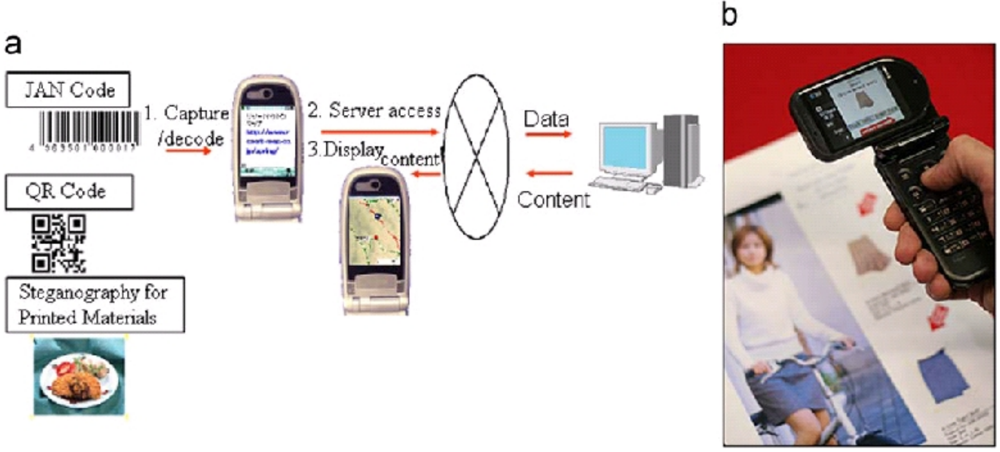


Fig. 2. Fujitsu exploitation of stteganography: (a) a sketch representing the concept and (b) the idea deployed into a mobile phone shown at an exhibition.

It also supports laws of information privacy where no one can disclose or misuse the private data of an individual either intentionally or unintentionally. These data can cover a wide range such as criminal investigation reports, biological traits, bank details and in military to transfer important information hiding it from enemies etc.

## III. ANCIENT METHODS OF STEGANOGRAPHY

The steganography has the existence of about thousands of years. It is originally derived from Greek words which has the meaning "Covered Writing". In the 5th century BC Histaiacus used the slave's head for hiding the message. He shaved the head, tattooed a message on his skull and then send him after his hair grew back [4, 6, 7]. Five hundred years ago, the Italian mathematician Jerome Cardanre invented a Chinese ancient method of secret writing. The process is as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as an innocuous text as shown in Fig. 3. This method is credited to Cardan and is called Cardan Grille [8].

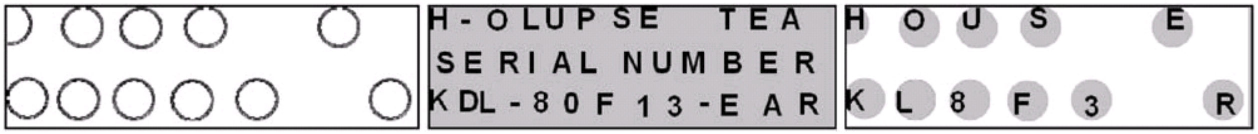


Fig. 3. Cardan Grille: an illustration, keeping in mind that the Grill has no fixed pattern: (Left) the mask, (middle) the cover and (right) the secret message revealed.

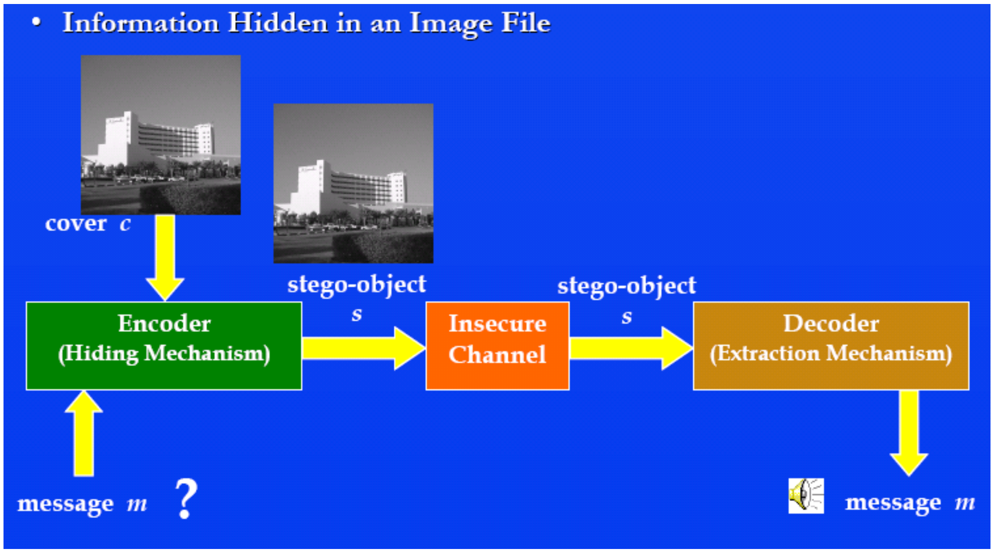
Nazis also invented several steganographic methods during World War II such as Microdots, and have reused invisible ink and null ciphers. As an example, a message was sent by a Nazi spy that read: "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils." Using the 2nd letter from each word the secret message reveals: ”“Pershing sails from NY June 1’’ [9, 10].

## IV. BASIC CONCEPTS OF STEGANOGRAPHY

The main idea behind steganography is to hide a message or an image behind another image as shown in Fig.4. Some of the popular image formats that are used on the internet to hide the secret message are graphics interchange format GIF), Joint Photographic Experts Group (JPEG), and to some extent is the portable network graphics (PNG). The process of embedding is explained by the Fig.5 where C denotes the cover image and C' the stego-image. Let K represent an optional key (a seed used to encrypt the message or to generate a pseudorandom noise which can be set to {Φ} for simplicity) and let M be the message we want to communicate. Em is an acronym for embedding and Ex for Extraction.

$$Em : C \times K \times M \rightarrow C' \qquad ...(1)$$

$$\therefore\ Ex(Em(c,\ k,\ m))\ \approx\ m,\ \forall\, c \in C,\ k \in K,\ m \in M$$



- Information Hidden in an Image File

...(2)

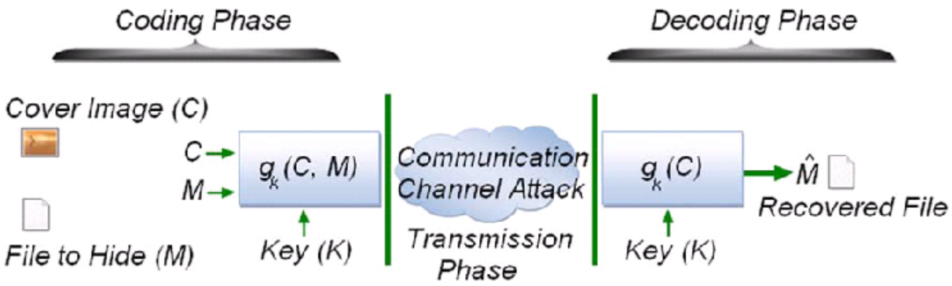


Fig. 4. View of the basic mechanism of data hiding.

Fig. 5. Communication-theoretical view of a generic embedding process: C denotes Cover image, M denotes the data to hide.

The core concept of digital image steganography is to hide the secret message in the pixels of the image. Each pixel is basically composed of three color components, Red, Blue and Green, each consisting of one byte. The ASCII values of the text messages are over written in the bits of these pixels. But by doing this, original image is distorted and intruder may easily guess that something is hidden here. So, in most of the cases, least significant bits of the pixels are used for hiding the text. Conventional steganography usually embeds the secret data into the least-significant bits (LSBs) of each pixel in the cover image [11, 12]. Such an approach is called the LSBs substitution method, which only slightly changes the original values without obvious perceptible distortion. Although a number of variants of the LSBs method have been proposed [13, 14], such tiny distortions are unacceptable to some sensitive applications, such as military and medical data. Therefore, how to design a lossless hiding method becomes a crucial issue. The lossless (also called reversible) steganographic method is a method by which the original cover image can be recovered completely from the stego-image after extraction of secret data. The basic mechanism of hiding data using LSB technique is shown in Fig.6.

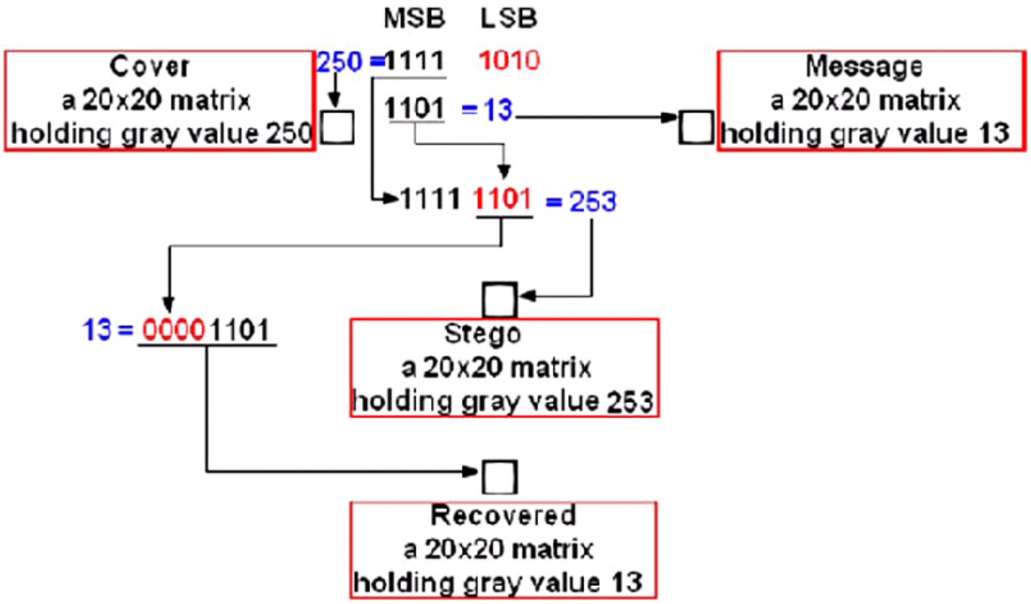


Fig. 6. Steganography in spatial domain. The effect of altering the LSBs up to the 4the bit plane.

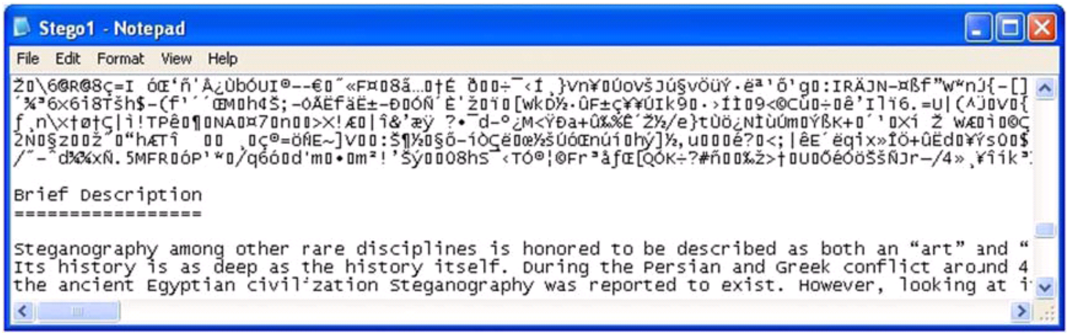
## V. METHODS USED IN DIGITAL IMAGE STEGANOGRAPHY AND REVIEWS

Starting era of scientific steganography can be marked as when people started appending data in the digital images by breaking the EOF (end of file) tag. This could be simply done by writing the following code in windows OS command window:

```
C:\> copy cover.jpg /b + msg.txt /b stego.jpg
```

This code appends the secret message written in the file "msg.txt" into the jpeg image file "cover.jpg" and produces the new image file "stego.jpg". The main idea is to break the EOF tag and insert the message after it [1]. When the stego.jpg is viewed by using any photo editing applications then it will just display the picture ignoring anything that comes after the EOF tag. But if it is opened in notepad then message will be revealed as shown in Fig.7. Thus, the text can be encrypted for making it more secure. The advantage of this method is that, it is very simple to hide the text message without causing any distortions in the image. That is, stego-image will be same as the cover image which does not remain same in other techniques like LSB that will be discussed later. Though this method produces the lossless stego-image but message can be extracted easily.

Steganography can also be implemented by appending data into the image's extended file information (EXIF), which is a standard used by digital camera manufactures to store information such as model of the camera, time when the picture was taken, focal length, resolution of the image etc. [15]. This method also suffers from the same drawback of EOF and therefore we should encrypt the data before hiding in it.



```
Ž□\6@R@8ç=I óŒ'ñ'Å¿ÙbóUI®--€□˜«F¤□8ã…□†É ð□□÷¯‹Í¸}Vn¥□ÚovšJú§vÖüÝ·ëª'õ'g□:IRÄJN–¤ßf"w*nĴ{-[]
´¾³6×6ì8Ťšh$-(f'´´ŒM□h¢Š;-óÅËfäË±-Ð□ÓÑ´È'Ž□ï□[wkÐ½·ûF±ç¥¥ÚIk9□·›Ì͏□9<©Cû□÷□ê'I1ï6.=U|(^Ĵ□V□{
ƒ¸n\×†ø†Ç|ì!TPê□¶□NA□¤7□n□□>X!Æ□|î&'æÿ ?•¯d-º¿M<ŸÐa+û%%Ê´Ž½/e}tÙö¿NÌùÚm□ÝßK+□´'□Xí Ž WÆ□ì□©Ç
2N□§z□□ž˝□"hÆTî  □□ ¸□ç®=öÑE~]V□□:Š¶½□§õ-íòÇë□œ½šÚóŒnúí□hý]½,u□□□é?□<;|êE´ëqix»ÎÖ+ûËd□¥Ÿs0□$
/˝-ˆd%%xÑ.5MFR□óP'*□/q6ó□d'm□•□m²!'Šý□□08hS¯‹TÓ®¦©Fr³åfŒ[QÓK÷?#ñ□□%ž>†□U□ŐéÓöŠšÑJr–/4»¸¥îík³:

Brief Description
=================

Steganography among other rare disciplines is honored to be described as both an “art” and “
Its history is as deep as the history itself. During the Persian and Greek conflict aroↄnd 4
the ancient Egyptian civilˈzation Steganography was reported to exist. However, looking at i
```

Fig. 7. The secret message revealed when the stego-image is opened using Notepad. Note that the format of the inserted message remains intact.

Shirali–Shahreza [16] used Arabic and Persian alphabet punctuations to hide messages but this technique is not related to the LSB approach. In Persian language, 18 alphabets out of 32 have dots and these dots are modified according to the values in the binary file.

Chin-Chen *et al*. [17] used run length ( RLE ) encoding technique that was initiated in 1950. They proposed two data hiding methods incorporating both run-length encoding and modular arithmetic. The first method, BRL (hiding bitmap files by run length), is for embedding simple data with long streams of repeating bits; the second method, GRL (hiding general files by run-length), is for embedding complicated data with short streams of repeating bits. They used two consecutive pixels of the cover image (gray-level image) for hiding the secret message. They also imposed the constraint on the secret message that it must consist of repeating characters.

RLE works by reducing the space occupied by strings of repeating characters. Such a string is usually referred to as a run, which is recorded by two symbols that form an RLE packet: (*i*) the run count, denoting the number of characters in the run, and (*ii*) the run value, indicating the common value of the characters in the run. For example, AAAAABBBBAA is encoded as 5A4B2A in the RLE system: 5, 4, and 2 are the run counts; A and B are the run values; and 5A, 4B, and 2A are the RLE packets. For the sake of convenience, the first and second pixels in each two-pixel block are denoted as vi and ci, respectively, whose stego-values are denoted as v'i and c'i. In general, messages of repeating characters has no meaning. Since they are using gray-scale images for hiding data, so embedding capacity will also be less. In meaningful messages, characters repeat very rare so complexity will also increase.

Xin Liao *et al*. [18] also used gray-scale images as the cover image and gave emphasis on finding the edge pixels of the cover image to hide the secret message because changes in these locations are least visible. They partitioned the image into smooth area and edge area by calculating the differences of gray values of 4-pixel block. They used 3-bit common LSB substitution method to hide the data. For eg., if data is $000_{(2)}$ and pixel p = $1100111_{(2)}$ then p'=$1100000_{(2)}$ and then they increased the MSB of p' by 1 *i.e*. p' = $1101000_{(2)}$ to reduce the difference between p and p'. For messages like 010, 001, 100 etc., they did not discuss at all about how to change the MSB of p'. They used very simple LSB method for embedding but involved many calculations to find smooth and edge areas to make it more complex and thus reducing the efficiency.

Hassan *et al*. [19] chose colored images for hiding the messages. They focused on selecting the pixels from the particular position of the image and then hided the message. They selected the pixels from the corner, center and quadrant wise in both the directions, that is clockwise and counter-clockwise as shown in fig.8 and fig.9. They hided only 3 bits in each pixel, that is, one bit in each of the RGB component of the pixel. Because of the selection procedure of pixels, clustering will occur. Some portions of the image will be heavily changed and some will not change at all. Since they embedded only 3 bits in each pixel, so embedding capacity will also be less and they did not discuss anything on making the data secure. When they showed the results, they only mentioned the algorithm number and did not mention anything about the algorithms.

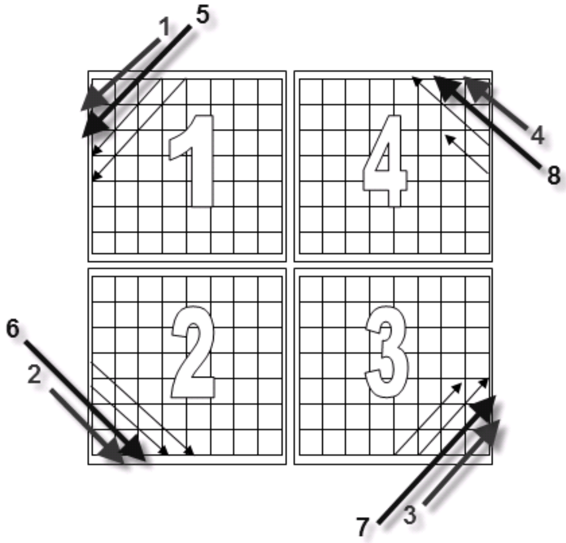


Fig. 8. Counter clock-wise direction from corner.

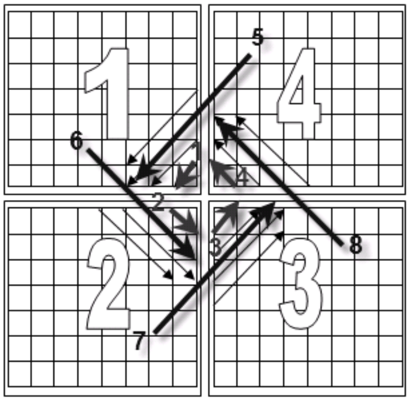


Fig. 9. Counter clock wise direction from center.

Another technique that is used for hiding data comes in the category of adaptive steganography. It aims to reduce modifications to the cover image, and adapts the message embedding technique to the actual content and features of the cover image. Adaptive methods embed a message bit into certain random clusters of pixels, avoiding areas of uniform color and select pixels with large local standard deviation or blocks containing a number of different colors. In StegoAdapt [20], the cover image is divided into 3×3 blocks of pixels, and the message bit is encoded as the parity of the central pixel in each pseudo randomly selected potential block. The block is considered to be suitable for bit storage if the central pixel in the block is different as compared to at least one of the surrounding pixels in the block. A suitable block may become unsuitable after bit storage so it is checked again after embedding. Since out of nine pixels, only one pixel is chosen for embedding if it is different from the surrounding pixels, this will lead to low embedding capacity.

Santosh Negi *et al*. [21] discussed a method that adaptively modifies the intensities of pixels obtained after filtering. These are the high frequency components spatial image pixels (HFSI) of the cover image. They modified the pixels to a large extent for hiding the message where the contrast of the image was large. And where the contrast was small (e.g., a smooth image), they only slightly tuned the intensities. The portion of the image which is already highly contrasted is chosen for further changes to hide the messages. The result can be guessed.

Bhattacharyya *et al*. [22] proposed three layer of security and used LSB method for steganography. At first, they encrypted the text message using some public and private key. This encrypted code is then converted into binary matrices whose size is dependent on the size of the depth of the cover image and size of the code that is obtained from the encryption procedure of the text. After this, they embedded the binary values of the obtained matrix into least significant bits of the cover image and left one or two pixels unchanged following some order when one complete word is embedded.

Ibrahim *et al*. [23] also embedded secret message through their steganography imaging system (SIS). They mentioned about two layer of security, first is the password for opening the system and second is hiding the message inside the image. They used a key to retrieve the message from the image. They only used the .bmp images for hiding the messages and did not discuss about the mechanism. Moreover, key is also embedded with the data in the cover image which might make a way simple to retrieve the secret message from the stego-image.

## VI. CONCLUSION

In this paper, we presented the basic concepts of implementing steganography in digital images. That is, how the pixels of the image are manipulated to store the secret message Fig 6. It also discusses some applications of steganography that varies from the privacy of an individual to the security of a nation. It is tried to maintain a link about the concepts of steganography from the origin to the latest techniques. It compares the differences between steganography, water marking and encryption. Steganographic techniques proposed by various scholars are reviewed, their summary is presented and brief comments are also stated. Xin Liao *et al*. [18] tried to reduce the differences between original pixel and stego-pixel where as Hassan Mathkour *et al*. [19] stressed on locating the pixels of the image for embedding and proposed to hide 3 bits in one pixel.

Most of the methods are using the concept of hiding bit values either in the 4th LSB or in the 1st LSB or using 1, 2 and 3 LSB of the RGB components of a pixel. Some extra parameters should be taken so that the process of hiding the bits in the RGB components become more secure and it does not leave a simple way to extract the message from the cover image.

## REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods, *Signal processing* **90:** (2010), pp. 727-752, 18 August, (2009).

[2] Jamil, T., Steganography: The art of hiding information is plain sight, *IEEE Potentials*, (1999).

[3] Wang, H & Wang, S, Cyber warfare: Steganography vs. Steganalysis, *Communications of the* ACM, **47:** 10, October (2004).

[4] Johnson, N.F., and Jajodia, S., Exploring steganography: seeing the unseen, *IEEE Computer* **31**(2): pp. 26-34(1998).

[5] Petitcolas, F.A.P., Introduction to information hiding, in: S. Katzen- beisser, F.A.P. Petitcolas (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood, (2000).

[6] Judge, J.C., Steganography: past, present, future. SANS Institute publication, /http://www.sans.org/reading_room/ whitepapers/ stenganography / 552.phpS, (2001).

[7] Provos, N., Honeyman, P., Hide and seek: an introduction to steganography, *IEEE Security and Privacy* **1**(3): pp. 32-44(2003).

[8] Moulin, P., and Koetter, R., Data-hiding codes, *Proceedings of the IEEE* **93**(12): 2083-2126(2005).

[9] Lyu, S., Farid, H., Steganalysis using higher-order image statistics, *IEEE Transactions on Information Forensics and Security* **1**(1): 111-119(2006).

[10] Kahn, D., The codebreakers: the comprehensive history of secret communication from ancient times to the Internet, Scribner, December 5, (1996).

[11] Bender, W., Gruhl, D., Morimoto, N., A. Lu, Techniques for data hiding, *IBM Syst. J.* **35**(3&4): pp. 313-336(1996).

[12] Chin-Chen Chang, Chih-Yang Linb, Yi-Hsuan Fan, Lossless data hiding for color images based on block truncation coding, *Pattern Recognition* **41:** Elsevier, pp. 2347-2357(2008).

[13] Y.H.Yu, C.C. Chang,Y.C. Hu, Hiding secret data in images via predictive coding, Pattern Recognition **38**(5): 691-705(2005).

[14] Chan, C.K., and Cheng, L.M., Hiding data in images by simple LSB substitution, Pattern Recognition **37**(3): 469-474(2004).

[15] Alvarez, P., Using extended file information (EXIF) file headers in digital evidence analysis, *International Journal of Digital Evidence, Economic Crime Institute* (ECI) **2**(3): 1-5(2004).

[16] Shirali-Shahreza, M.H., and Shirali-Shahreza, M., A new approach to Persian/Arabic text steganography, in: *Proceedings of Fifth IEEE/ACIS International Conference on Computer and Information Science* (ICIS-COMSAR 2006), 10-12 July, p: 310-315(2006).

[17] Chin-Chen Chang, Chih-Yang Lin, Yu-Zheng Wang, New image steganographic methods using run-length approach, *International Journal of Information Sciences* (176), Elsevier, 03 February, p: 3393-3408(2006).

[18] Xin Liao, Qiao-yan Wen, Jie Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution, Journal of Vis. Commun. Image R 22 (2011), Elsevier, **22:** Aug, p: 1-8(2010).

[19] Hassan Mathkour, Ghazy M.R. Assassa, Abdulaziz Al Muharib, Ibrahim Kiady, A Novel Approach for Hiding Messages in Images, International Conference on Signal Acquisition and Processing, *IEEE computer society*, 10 Nov, p: 89-93(2009).

[20] Karen Bailey, Kevin Curran and Joan Condell, An Evaluation of Pixel based Steganography and Stegodetection Methods, *The Imaging Science Journal*, Vol **52**(3): 131-150, September (2004).

[21] Santosh, N. Arjun, Atul Negi, A High Embedding Capacity Approach to Adaptive Steganography, 1-4244-0682-X/06/ $20.00 © IEEE, p: 525-530(2006).

[22] Bhattacharyya, Debnath Poulami Das, Samir Kumar Bandyopadhyay, Tai-hoon Kim, Text Steganography: A Novel Approach, *International Journal of Advanced Science and Technology* Vol. 3, pp. 79-86, February, (2009).

[23] Ibrahim Rosziati and Teoh Suk Kuan, Steganography algorithm to hide secret message inside an image, *Journal of Computer Technology and Application* **2:** (2011), 25 Feb, pp. 102-108(2011).