*International Journal of Innovative Research in Electronics and Communications (IJIREC)*
*Volume 1, Issue 1, April 2014, PP 1-12*
*www.arcjournals.org*

# High Capacitive and Confidentiality Based Image Steganography and Watermarking using Private Stego-Key

**Humera Sheikh**
M.Tech, Dept. of Electronics,
Wainganga College of Engg. & Management,
Nagpur, India
*hshumera1@gmail.com*

**Abstract:** *Steganography and watermarking are two important areas of research and it involve a number of applications. These two areas of research are important especially when reliable and secure information exchange is required. Steganography methods usually do not need to provide strong and safe security against removing or modification of the hidden message. Watermarking methods need to be very robust to attempts to remove or modify a hidden message. A data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional useful data. With an encrypted image containing additional data, if a receiver has the data-hiding key, then he can able to extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error. To enhance the embedding capacity of image steganography and watermarking for human vision, a novel adaptive number of least significant bits substitution method with private stego-key based on gray-level ranges is proposed in this paper.*

**Keywords:** *Steganography, Watermarking, Data hiding, Cover-image, LSBs, stego-key.*

## 1. INTRODUCTION

One of the most important property of (digital) information is that it is in principle very easy to produce and distribute unlimited number of its copies. This might undermine the music, film, book and software industries and therefore it brings a variety of important problems concerning the protection of the intellectual and production rights that badly need to be solved. The fact that an unlimited number of perfect copies of text, audio and video data can be illegally produced and distributed requires to study ways of embedding copyright information and serial numbers in audio and video data. Steganography and watermarking bring a variety of very important techniques how to hide important information in an undetectable and/or irremovable way in audio and video data. Steganography and watermarking are main parts of the fast developing area of information hiding. Differences between steganography and watermarking are both subtle and essential. The main goal of steganography is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot detect the presence of m in d'. The main goal of watermarking is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically

indistinguishable from d, by people, in such a way that an eavesdropper cannot remove or replace m in d'. It is also often said that the goal of steganography is to hide a message in one-to-one communications and the goal of watermarking is to hide message in one-to-many communications. Shortly, one can say that cryptography is about protecting the content of messages, steganography is about concealing its very existence. Steganography methods usually do not need to provide strong security against removing or modification of the hidden message. Watermarking methods need to be very robust to attempts to remove or modify a hidden message.

**Digital Watermarking:** Digital watermarking is changing an image in a way so that you can see some text or background image without actually corrupting the image [2].

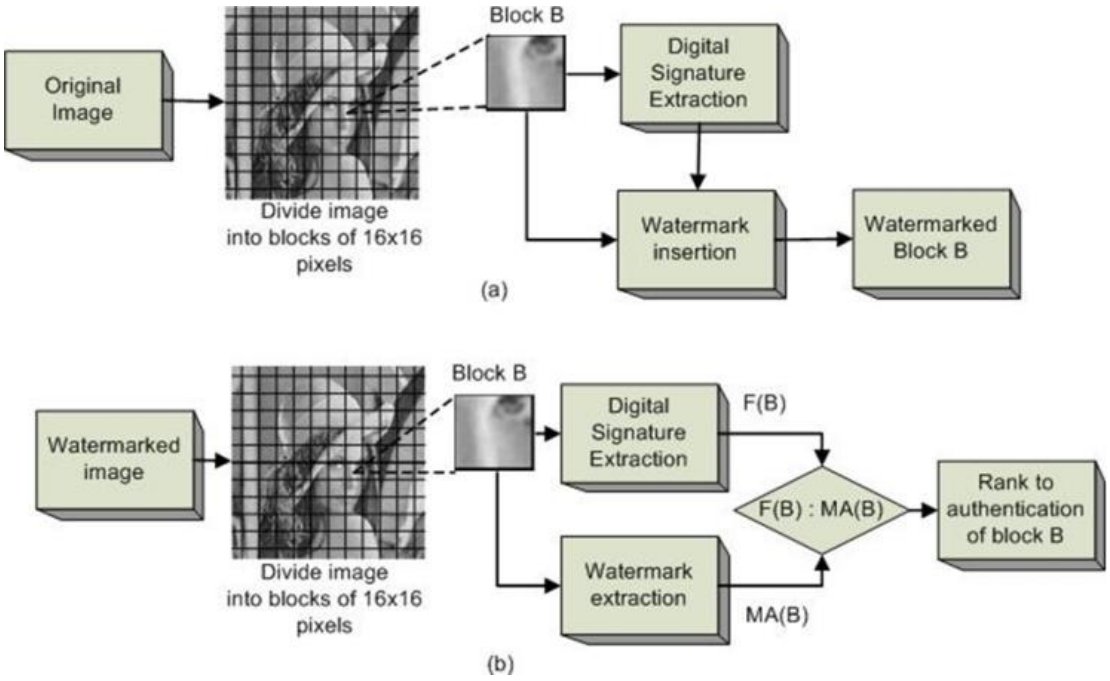


**Fig 1.** *a) Watermark insertion system; (b) Watermark extraction system. [2]*

**It's Applications:**

- It is used for copyright protection.
- It is used for source tracing.
- Annotation of photographs.

**Steganography:** Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected [2].

These different categories can be specified as follows:

- Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.
- Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes.
- Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the

positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or hand written text.

- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.

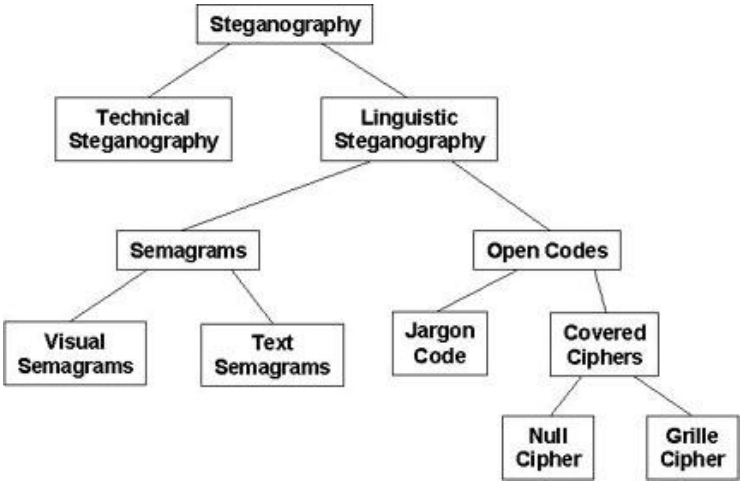


**Fig 2.** *Steganography and its techniques [2]*

- Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal, underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.
- Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word [3]."

**Basic steganographic techniques:**

Substitution techniques substitute redundant part of the cover-object with a secret message.

Spread spectrum techniques embed secret messages adopting ideas from spread spectrum communications.

Statistical techniques embed messages by changing some statistical properties of the cover-objects and use hypothesis-testing methods in the extraction process.

Distortion techniques store secret messages by signal distortion and measure the deviation from the original cover in the extraction step.

Cover generation techniques do not embed messages in randomly chosen cover objects, but create covers that fit a message that need to be hidden.

## 2. REVIEW OF RELATED WORK

The usage of a stego –key is important, because the security of a protection system should not be based on the secrecy of the algorithms itself, instead of the choice of a secret key [13]. The steganographer's job is to make the secretly hidden information difficult to detect given the complete knowledge of the algorithm used to embed the information except the secret embedding key. This so called kerckhoff's principle is the golden rule of cryptography and is often accepted for steganography as well [15]. Some steganographic methods [16] [17] uses a stego-key to embed message for achieving rudimentary security. Beenish et al. [5] proposed technique uses predictive position agreed between two parties as stego-key. Same position used only once to enhance security. But drawback of the algorithm is small amount of data to be embedded.

The most common and simplest steganographic method [18] [19] is the least significant bit insertion method. It embeds message in the least significant bit. For increasing the embedding capacity two or more bits in each pixel can be used to embed message. At the same time not only the risk of making the embedded statistically detectable increase but also the image fidelity degrades. So how to decide the number of bits of each pixel used to embed message becomes an important issue of image steganography. S.K. moon and R.S. kavitkar [23] proposed a fixed 4LSB method to embedding an acceptable amount of data; 4LSB embedding data can easily be implemented and do not visually degrade the image to the point of being noticeable. But drawback of the scheme is that the encoded message can be easily recovered and even altered by 3rd party. So techniques must be developed to solve above said problems. Lie et al. [24].proposed an adaptive method based on using variable amount of bits substitution instead of fixed length for adjusting the hiding capacity. Abbas cheeldod et al. [20] proposed an adaptive steganography that select the specific region of interest (ROI) in the cover image. Where safely embeds data. The choice of these regions based on human skin tone color detection. Adaptive steganography are not an easy target for attacks especially when the hidden message is small [21]. The tri-way pixel value differencing method proposed by ko-chin-chang can successfully provide embedding capacity and outstanding imperceptibility for the stego-images. K. Suresh Babu et al. [22]. Proposed steganographic model authentication of secret information in image steganography, that can be used to verify the integrity of the secret message from the stego-image .In this method payload is transformed from spatial domain to discrete wavelet transform. The DWT coefficients are then permuted with the verification code and then embedded in the special domain of the cover image. The verification code is generated using to special coefficient in the DWT domain. Thus the method can verify each row has been modified or forget by attacker.

## 3. PROPOSED TECHNIQUE

The proposed scheme works on the spatial domain of the cover image and employed an adaptive number of least significant bits substitution. Variable K-bits insertion into least significant part of the pixel gray value is dependent on the private stego-key K1 .Private stego-key consists of five gray-level ranges that are selected randomly in the range 0-255. The selected key shows the five ranges of gray levels and each range substitute different fixed number of bits into least significant part of the 8-bit gray value of the pixels .After making a decision of bits insertion into different ranges. Pixel p(x, y) gray value "g" that fall within the range Ai-Bi is changed by embedding k-message bits of secret information into new gray value "g' ". This new gray value "g' "of the pixel may go beyond the range Ai-Bi that makes problem to extract the correct information at the receiver. Specific gray value adjustment method is used that make the new gray value "g' " fall

within the range Ai-Bi. Confidently is provided by the private stego-key and to provide integrity of the embedded secret information, 140-bit another key K2 is used. Digital signature of the secret information with the key is find and appended with the information .The whole message plus signature is embedded into the cover image that provide some bit overheads but used to verify the integrity .At the receiver key K1 is used to extract the message and key K2 is used to verify the integrity of the message.

**Private stego-key generation:** Private stego-key K1 play an important role in proposed scheme to provide security and deciding the adaptive K bits insertion into selected pixel. For a gray scale images 8-bit used to represent intensity of pixel, so there are only 256 gray values any pixel may hold. Different pixels in images may hold different gray values .We may divide the pixels of images into different groups based on gray ranges .Based on this assumption let five ranges of gray levels are < A1-B1 , A2-B2 , A3-B3 , A4-B4 , A5-B5 > each range starting and ending value are in 8-bits, total 80-bits are used to make a key K1. If the difference of each range is denoted by Di=Bi-Ai, it should not be less than 32 gray values and any range should not be overlap with other ranges.

**Method to decide Bits insertion into each range:** Let the five gray ranges decided by the stego-key are <A1-B1,A2-B2,A3-B3, A4-B4 ,A5-B5 > and number of pixel count from cover image in each range are <N1,N2,N3,N4,N5>. After counting the number of pixel in each range we fixed the number of bits insertion into each range according to the rule given below.

3 Bits subs. (Max. Pixel count range)

2 bits subs (Second max count)

R (i) = 3 bits subs. (Third max. count)

4 bits subs. (Second min. count)

5 bits subs. (Min. count)

Where R(i) denote the range and value of i is within the range $1 \leq i \leq 5$;

In the similar way from the stego-image we decide the bits extraction.

**LSB Substitution:** Least significant substitution is an attractive and simple method to embed secret information into the cover media and available several versions of it. We employ in propose scheme adaptive LSB substitution method in which adaptive K-bits of secret message are substituted into least significant part of pixel value.

To decide arbitrary k-bits insertion into pixel, first we find the range of pixel value and then find the number of bits insertion and insert K-message bits into least significant part of pixel using LSB. After embedding the message bits the changed gray value g' of pixel may go beyond the range. To make value within the range, reason is that receiver side required to count pixels to extract message, pixel value adjusting method is applied to make changed value within range.

**Pixel value adjusting method:** After embedding the K-message bits into the pixel gray value g new gray vale g' may go outside the range .For example let our range based on key is 0-32. The gray value g of the pixel is 00100000 in binary form (32 in Dec.).decided K-bits insertion is 3-bits are 111.The pixel new gray value g' will be after insertion in binary is 00100111 (39 in Dec).Modified value is outside the range .To make within the range 0-32, K+1 bits of g' is changed from 0 to 1 or via- versa. And checked again to fall within range if not K+2 bit is

changed and so on until gray value fall within range. For above example. 00100111 - 00101111 - 00111111-00011111.

**Digital signature:** To verify the integrity of the stego-image and secret information, a simple Ex-OR method to find signature of secret message with random stego-key of 140 bits is used and appended with the message, some overheads occurs but integrity of the message is checked at the receiver.

**Finger Printing & Watermarking Method:** These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge but sometimes it may even be visible, while in steganography the imperceptibility of the information is crucial. A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the

mark, but to remove it[4].

In watermarking modifications of contents by adding identification data while in fingerprinting contents are not affected.

- Watermarking allow the precise identification of each piece of content and in fingerprinting work for legacy content.
- Watermarking stand alone and fingerprinting connection to database required.

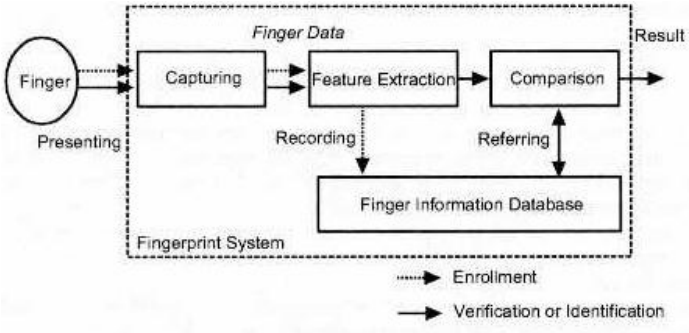


**Fig.3** *Fingerprinting Process [2]*

## 4. USES OF WATERMARKING

A Watermark is a form, image or text that is impressed onto paper, which provide evidence of its authenticity. Digital Watermarking is an extension of this concept in the digital world. In recent years the phenomenal growth of the internet has highlighted the need for mechanism to protect ownership of digital media. Digital Watermarking is a technique that provides a solution to the longstanding problems faced with copyrighting digital data. For following applications we used digital watermarking:-

Ownership assertion: Watermarking is used to establish ownership over the content.

Authentication and integrity verification: - content which is protected by key verification should not be accessible without authentication.

Usage control: To limit copies creation of copyrighted data, by blocking using watermark.

Content labeling: Bits embedded in data giving extra information.

## 5. USES OF STEGANOGRAPHY

Steganography has a wide array of uses. It can be used for digital watermarking, ecommerce, and the transport of sensitive data. Digital watermarking involves embedding hidden watermarks, or identification tokens, into an image or file to show ownership. This is useful for copyrighting digital files that can be duplicated exactly with today's technologies [4]. 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 e-commerce transaction verification [4]. Unfortunately, steganography can also be used for illegitimate reasons. For instance, if someone was trying to steal data, they could conceal it in another file or files and send it out in an innocent looking email or file transfer. As was pointed out in the concern for terroristic purposes, it can be used as a means of covert communication.

### Overview

In this project we are introducing an enhancement of the gray-scale image ADAPTIVE steganographic system using LSB (LEAST SIGNIFICANT BIT) to get a security for the personal data and communication. In order to have a high security to the personal data we are using an key which we have given a name called stego- key. A variable bits stego-key has been applied to the system during embedment of the message into the cover image. Here in the algorithm is given that we can embed the message bits adaptively into the cover-image pixels instead of sequentially. Protect secret message from being stolen during transmission, there are two ways to solve this problem in general. One way is encryption and second way is invisibility.

The technique embeds the hidden information in the spatial domain of the cover image and uses simple (Ex-OR operation based) digital signature using a variable -bit key to verify the integrity from the stego-image. Besides, the embedded confidential information can be extracted from stego-images without the assistance of original images. By using the stego key we are getting the high security and by adaptive stegnography data invisibility is high. By taking advantage of human perception it is possible to embed data within a file. For example, with audio files frequency masking occurs when two tones with similar frequencies are played at the same time. The listener only hears the louder tone while the quieter one is masked. Similarly, temporal masking occurs when a low-level signal occurs immediately before or after a stronger one as it takes us time to adjust to the hearing the new frequency. This provides a clear point in the file in which to embed the mark. However many of the formats used for digital media take advantage of compression standards such as MPEG to reduce file sizes by removing the parts which are not perceived by the users. Therefore the mark should be embedded in the perceptually most significant parts of the file to ensure it survives the compression process. Clearly embedding the mark in the significant parts of the file will result in a loss of quality since some of the

information will be lost. A simple technique involves embedding the mark in the least significant bits which will minimize the distortion. However it also makes it relatively easy to locate and remove the mark. An improvement is to embed the mark only in the least significant bits of randomly chosen data within the file.

In this section a number of different information hiding techniques will be discussed and examined. The media involved vary from images to plain text. While some techniques may be used to hide a certain type of information, in most cases different information can be hidden depending on space restraints.

**Binary File Techniques**

If we are trying to hide some secret information inside a binary file, whether the secret information is a copyright watermark or just simple secret text, we are faced with the problem that any changes to that binary file will cause the execution of it to alter. Just adding one single instruction will cause the executing to be different and therefore the program may not function properly and may crash the system.

## 6. METHODOLOGY

1) We will study first the basic implementation of stegnography and water marking for encryption of secret messages.
2) First we will implement the stegnography for hiding encrypted image with text the data hidden in the form of text will be hidden with images. So, the data hidden in image is called as stegno-image.
3) Similarly the data in the form of image is encrypted or hidden or imbedded is to be retrieved back so as to decrypt the hidden image, so to embed image on image we will use water marking technique.
4) Here percentage of watermarking & stegnography is commonly used by using same algorithm using LSB.

## 7. RELATED RESEARCH

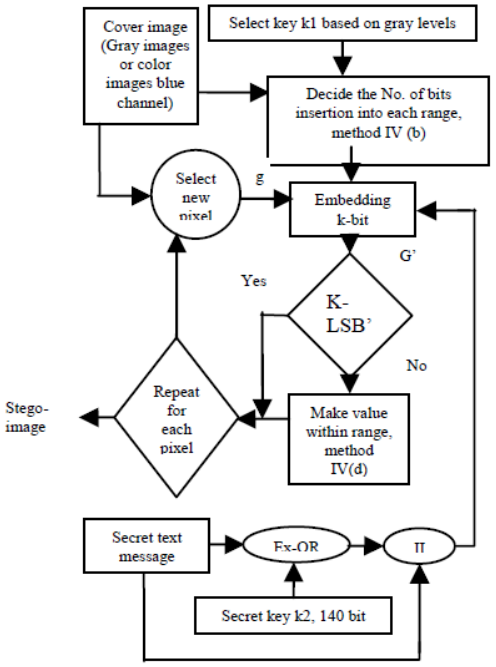


**Fig 3.***Message embedding with signature*

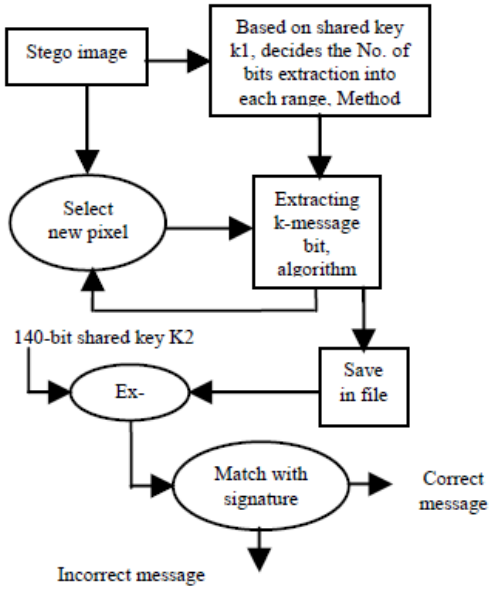


**Fig. 4** *Message extraction and integrity check*

## 8. PROPOSED ALGORITHMS

Input: - Cover-image, secret message, keys K1, K2.

Output: - Stego-image.

Step1: Read the key K1 first which based on gray-Level ranges.

Step2: To read cover image.

Step3: Decide No. of bits insertion into each range.

Step4: Read the secret message and Convert it into bit stream form.

Step5: Read the key K2.

Step6: Find the signature using K2 and append with the message bits.

Step7: For each Pixel

7.1: Find gray value g.

7.2: Decide the K-bits insertion based on gray ranges.

7.3: Find K-message bits and insert it.

7.4: Decide and adjust new gray Value g.

7.5: Go to step 7.

Step8: End

### *A. Algorithm*

Input: Stego-image, keys K1, K2;

Output: Secret information;

Step1: Read key K1 based on gray-level ranges.

Step2: Read the stego image

Step3: Decide No. of bits extraction into each range.

Step4: For each pixel, extract the K-bits and save into file.

Step5: Read the key K2 and find the signature of bit stream

Step6: Match the signature.

Step7: End.

## 9. CONCLUSION

Steganography has its vital place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked. Digital Watermarking is more secure and easy method of data hiding .All techniques of data hiding secure data with their methods, but watermarking is more capable because of its efficiency and accuracy. In Watermarking we mark the information which is to be hiding. Security of data is essential today because of cyber-crime, which is highly increased day by day. Watermarking provide us easy and efficient and reliable security solutions of digital data. Watermarking provide security of not only images, but also audio video and text.

## REFERENCES

[1] Dr.V.Khanaa, Dr.Krishna Mohanta, "Secure And Authenticated Reversible Data Hiding In Encrypted Images",International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 3 March 2013, Page No. 558-568

[2] Gurpreet Kaur, Kamaljeet Kaur, "Digital Watermarking and Other Data Hiding Techniques", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013

[3] D.R.Denslin Brabin, Dr.J.Jebamalar Tamilselvi, "Reversible Data Hiding: A Survey", International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2013

[4] Pradeep Kumar Saraswat, Dr. R. K. Gupta, "A Review of Digital Image Steganography", Journal of Pure and Applied Science & Technology, Vol. 2(1), Jan 2012, pp. 98-106

[5] Nan-I Wu and Min-Shiang Hwang, "Data Hiding: Current Status and Key Issues", International Journal of Network Security, Vol.4, No.1, PP.1–9, Jan. 2007

[6] F.A.P Petitcolas, R.J. Anderson and M.G. Kuhn; "Information Hiding a Survey", Proceedings of the IEEE, vol.-87, issue 7, pp. 1062-1078, 1999.

[7] S. Dumitrescu, W. X. Wu and N. Memon , " On steganalysis of random LSB embedding in continuous-tone images", Proc. International conference on image Processing, Rochester, NY, pp.641-644, 2002

[8] Beenish Mehboob and Rashid Aziz Faruqui, "A steganography Impleme -ntation", IEEE-Symposium on Biometrics & Security technologies, ISBAST' 08, 23-24, April, 2008 Islamabad.

[9] K. Ahsan, & D. Kundur , "Practical data hiding in TCP/IP", Proceeding of the workshop on multimedia security at ACM multimedia,2002.

[10] A. Westfeld, "F5-A steganographic algorithm: High capacity Despite Better Steganalysis", Proc.4th Int'l Information Hiding. Workshop, Springer, verlag vol . 2137 , New York,2001

[11] Johnson, F. Neil, and Sushil Jajodia. "Exploring Steganography: Seeing the Unseen", Vol. 31, issue 2, .IEEE computer Feb. 1998, pp 26-34.

[12] D.E.Denning , E .Dorothy .“ Information Warfare and Security”. Boston , MA:ACM Press,1999: pp.310-313.

[13] Jian Zhao, E. Koch. “Embedding Robust Labels Into Images for Copyright Protection”, Proc. of the int’l Conf. on Intellectual property Right for specialized information, Knowledge and New Technologies, Vienna August 1995.

[14] I. Cox, J. Kilian, T. Leighton and T. Shamoon, “Secure spread spectrum watermarking for multimedia”. IEEE Transation On Image processing, Vol 6, issue 12 , pp1673-1687,1997.

[15] Jiri Fridrich .“ A New Steganographyic Method for Palette-Based Images”. Center for Intelligent Systems, SUNY Binghamton, Binghamton, NY 13902-6000. U.S Government, a grant number F30602-98-c-0009.

[16] R.J. Anderson. and F.A.P. Petitcolas ,“On the Limit of Steganography ” .IEEE J. Sel . Areas Communication. vol 16 ,(4), pp.474-481,1998.

[17] M.Kutter, E. Jordan, and E. Bossen ; “Digital signature of Color images using amplitude modulation”, J. Electron Imaging , vol. 7, (2),pp.326-332,1998.

[18] E.T. Lin, E.J. Delp. “A review of data hiding in images”. , Proceedings of the conference on image processing image quality image capture systems, PICS’99’. 25-28, April 1999, savannah, Georgia, pp. 274-278

[19] BENDER, W. GRUHL, D. MORIMOTO N, and A. LU, “Techniques for data Hiding”, IBM, syst. J., 35, (3&4) pp.313-336,1996.

[20] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt’:“Enhancing Steganography in digital images”.IEEE-2008 Canadian conference on computer and Robot vision, pp.326-332.

[21] KO-Chin Chang, Chien-Ping Chang, Ping S.Huang,and Te-mingTu.:“ A novel image steganographic method using Tri-way pixel value Differencing”.Journal of multimedia, Vol.3,No.2,June-2008.

[22] K.Suresh Babu , K. B . Raja , Kiran Kumar k , Manjula Devi T H , Venugopal K R ,L . M Patnaik . : “Authentication of secret information in image steganography;”TENCON-2008, IEEE Region 10 Conference. pp. 1-6, Nov 2008.

[23] S. K. Moon and R.S. Kawitkar, “Data Security using Data Hiding”, IEEE International conference on computational intelligence and multimedia applications, vol. 4, pp. 247-251, Dec. 2007.

[24] W. N. Lie and L. C. Chang, “ Data Hiding in images with adaptive numbers of least significant bits based on human visual system”, IEEE international conference on image processing, vol.-1, pp. 286-290, 1999.

[25] Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng and Zhang Xiong, (2010), “Reversible Image Watermarking Using Interpolation Technique”, IEEE Transaction on Information Forensics and Security, Vol. 5, No. 1, pp 187 – 193.

[26] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar ,(2010), “A Novel Technique for Image Steganography Based on Block-DCT and Huffman Encoding”, International Journal of Computer Science and Information Technology, Vol. 2, N0. 3, pp. 103-112.

[27] Neminath Hubballi and Kanyakumari D P,(2009), “Novel DCT based watermarking scheme for digital images”, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, pp. 430-43.

[28] Niels Provos and Peter Honeyman,(2003), “Hide and Seek: An Introduction to Steganography” , IEEE Security & Privacy, pp.32-44.

[29] Shaowei Weng, Yao Zhao, Jeng-Shyang Pan and Rongrong Ni,(2008), "Reversible Watermarking Based on Invariability and Adjustment on Pixel Pairs", IEEE signal processing letters, Vol. 15, pp. 721-724.

[30] Tsz Kin Tsui, Xiao-Ping Zhang Androutsos, (2008), "Color Image Watermarking Using Multidimensional Fourier Transforms" , IEEE Transactions on Information Forensics and security, Vol. 3, pp.16-28.