ISSN: 2321-7782 (Online)
Volume 3, Issue 1, January 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Visual Cryptography and Steganography: A Review

Pradnya S. Nagdive[1]
ME, CSIT dept.
H.V.P.M. College of Engg.
Amravati, India

A. B. Raut[2]
HOD, CSE dept.
H.V.P.M. College of Engg.
Amravati, India

Abstract: ***To maintain the privacy and certainty of pictures may be a spirited space of analysis, with two totally different approaches being followed, the primary being encrypting the pictures through encoding algorithms using keys, the secondary approach involves hiding the data using data hiding algorithms to take care of the pictures secrecy.***

A content owner encrypts the first image using an encoding key, and an information-hider will embed further data into the encrypted image employing a data-hiding key although he doesn't recognize the first content. With an encrypted image containing further information, a receiver could initially decode it with the encoding key, then extract the embedded information and recover the first image with the data-hiding key.

Keywords: Cover image, Information concealing, Information extraction, Image encoding, Image decoding, Information recovery.

I. INTRODUCTION

The security of information is presently one in every of the foremost pressing problems to that several researchers have paid plenty of attention. The visual cryptography (VC) planned by Naor and Shamir [2] could be a technique that safely shares a secret image to several participants. A (k,n) VC theme encodes a secret image into noise-like shares (called transparencies or shadows). Any k or a lot of shares visually reveal the key image after they area unit superimposed along. Whereas any smaller than k shares disclose no data of the key image. The charm of VC is that the decryption method needs neither machine device nor cryptological information, and therefore the secret image is reconstructed simply via the human sensory system. Hence, for the applications during which the computing devices for secret writing don't seem to be on the market or too expensive, VC becomes a reliable and handy technique to accomplish the sharing of digital pictures. However, the VC technique would be abundant enticing if a lot of data is hidden at intervals the cryptography method.

Visual cryptography could be a special kind of secret sharing during which the key is a picture and therefore the shares area unit random trying pictures written on transparencies. The fascinating peculiarity of this sort of secret sharing is that the reconstruction of the key is performed with nonemachine machinery: it's enough to superpose the shares (transparencies) so as to reconstruct the key. Visual cryptography has been introduced by Naor and Shamir in 1994. Kafri and Keren have introduced an identical technique, known as random grid coding, in 1987.

Cryptography could be a technique for securing the key data. Sender encrypts the message with the help of key then sends it to the receiver. The receiver decrypts the message to obtain the private data. Cryptography focuses on keeping the content of the message secret wherever as information concealing concentrates on keeping the existence of the message secret [1].Information Concealing is another technique for secured communication. Information Concealing involves hiding the data thus it seems that no data is hidden in the slightest degree. If an individual or persons views the item that is hidden within he or she's going to haven't any concept that there's any hidden information, so the person won't commit to rewrite the knowledge [2]. Information Concealing is the method of hiding a secret message at intervals cowl medium like image, video, text, audio.

Hidden image has several applications, particularly in today's fashionable, hi-tech world. Privacy and secrecy could be a concern for many folks on the net. Hidden image permits for two parties to speak on the secretly and covertly.

The strength of information activity gets amplified if it combines with cryptography. The terminologies utilized in Information Concealing are cover-image, hidden image, secret message, secret key and embedding rule. Cover-image is that the carrier of the message like image, video or audio file. Cover-image carrying the embedded secret data (information) is that the hidden image. Secret message is the data that's to be hidden in an exceedingly cowl image. The secret key is accustomed to insert the message reckoning on the hiding rule [2]. The embedding rule is that the means, that is employed to insert the key data within the cowl image.

The security of the transformation of hidden information is obtained by two ways: encoding and information concealing. A mixture of these two techniques is accustomed to increase the information security. In encoding, the message is modified in such a simplest way in order that no information is disclosed if it's received by associate degree assailant. Whereas in Information Concealing, the key message is embedded into a picture usually known as cowl image, then sent to the receiver. World Health Organization extracts the key message from the duvet message. Once the key message is embedded into cowl image then it's known as a hidden image [6]. The visibility of this image mustn't be distinguishable from the duvet image, in order that it virtually becomes not possible for the assailant to find any embedded message.

In 1995, Naor and Shamir introduced a really attention-grabbing and easy scientific discipline technique known as visual cryptography to guard secrets [11].Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images.

Visual cryptography is a cryptographic technique in which visual information (Image, text, etc) is encrypted in such a way that the decryption can be performed by the human visual system without need of computers [1]. Likewise other multimedia components, image is sensed by human. Pixel is the smallest unit that constructs a digital image. Each pixel of a 32 bit digital color image are divided into four parts, named as Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency. A 32 bit sample pixel is represented in the following figure.

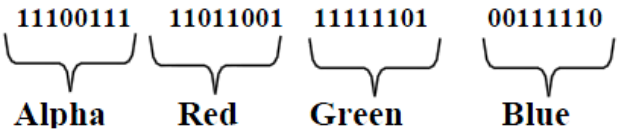

Fig 1: Structure of a 32 bit pixel

Human visual system acts as an OR function. Two transparent objects stacked together, produce transparent object. But after changing any of them to non-transparent, final objects will be seen non-transparent. In k-n secret sharing visual cryptography scheme an image is divided into n number of shares such that minimum k number of shares is sufficient to reconstruct the image. The division is done by Random Number generator [4]. This type of visual cryptography technique is insecure since the reconstruction is done by simple OR operation.

Basically, visual cryptography has two necessary options. The primary feature is its excellent secrecy and therefore the second is its decoding technique which needs neither complicated decoding algorithms nor the help of computers. It uses solely human sensory system to spot the key from the stacked image of some approved set of shares. Therefore, visual cryptography may be terribly convenient thanks to defend secrets once computers or alternative decoding devices aren't out there. The easy decoding technique is that the reason that pulls several analyzers to form additional elaborate enquiries during this research space. Nowadays, several connected ways regarding the speculation and therefore the applications of visual cryptography square measure planned.

An extended visual cryptography theme (EVCS) was planned by Ateniese et al. [12]. Extended visual cryptography schemes permits the development of visual secret sharing schemes inside that the shares square measure meaning as hostile having random noise on the shares. Once the sets of shares square measure superimposed, this meaning info disappears and therefore the secret is recovered. This is often the premise for the extended variety of visual cryptography [13-14]. The image size invariant visual cryptography was planned by Ito et al. [15]. The standard visual cryptography schemes use component enlargement. In component enlargement, every share is m times the scale of the key image. Thus, it will result in the issue in carrying these shares and consumption of additional space for storing. Ito's theme removes the necessity for this component enlargement. That is, the reconstructed image is the image of the initial image. There are also other studies that target the ways while not component enlargement.

In order to produce excellent secrecy and therefore the most clarity of the recovered secret pictures, most researchers use the thought of component enlargement, which was initialy introduced by Naor and Shamir to style their visual cryptography schemes. That is, every component of the binary secret image is encoded into m subpixels on every share, wherever m is termed the parameter of component enlargement of the theme. By analyzing any block of m subpixels of the tabu set of shares, one cannot distinguish that color was employed in the key component. however once the shares of the qualified set square measure stacked up, the block of any m subpixels equivalent to a black secret component can offer additional black subpixels than a block of subpixel equivalent to a white secret component. Thus, the blocks equivalent to black secret pixels can have additional blackness and people blocks equivalent to white secret pixels can have less blackness. This property makes it potential for somebody to tell apart black and white blocks, and therefore the key image will reveal the stacked image by losing some distinction of the initial secret image.

In 1996, Naor and Shamir planned an alternate VCS model for up the distinction in [3]. In 1999, Blundo et al. analyzed the distinction of the reconstructed image in k-out-of-n VCS schemes.

Blundo et al. gave a whole characterization of 2-out-of-n VCS schemes having best distinction and minimum component enlargement in terms of sure balanced incomplete block styles. Blundo et al.'s analysis results square measure valuable for the researchers United Nations agency have an interest within the space of visual cryptography. The opposite analysis works done by completely different authors square measure.

Viet and filmmaker planned a VCS with reversing, during which the participants also are allowed to reverse their transparencies. However during this theme there's a loss of resolution, since the amount of pixels within the reconstructed image is larger than that within the original secret image. Alternative studies associated with VCS with reversing square measure found in. The thought of algorithmic activity of secrets in visual cryptography was planned by Gnanaguruparan and Kak. This provides a technique of activity secrets recursively within the shares of threshold schemes, which allows AN economical utilization of knowledge. In algorithmic activity of secrets, many further messages are often hidden in one in every of the shares of the initial secret image. By using algorithmic threshold visual cryptography in network application, network load are often reduced.

Recently, visual cryptography schemes were conjointly planned to influence gray-level pictures. The employment of halftoning techniques create its potential that the readymade schemes designed for binary secret pictures are often directly applied to gray-level pictures. The various gray-level visual cryptography schemes square measure studied by researchers.

Applying visual cryptography techniques to color pictures may be a vital space of analysis as a result of it permits the employment of natural color pictures. Color pictures also are extremely standard and have a wider vary of uses when put next to alternative image sorts.

In 1997, Verheul and Van Tilborg planned a coloured visual cryptography theme. In 2000, principle and Laih planned a distinct construction mechanism for the coloured visual cryptography theme. They argued that their technique are often simply

enforced and may get far better block length than Verheul and Van Tilborg's theme. a significant common disadvantage of the on top of reviewed coloured VCS schemes is that range|the amount|the quantity} of colours and therefore the number of subpixels verify the resolution of the discovered secret image. If several colours square measure used, the subpixels need an oversized matrix to represent it. Also, the distinction of the discovered secret image can go down drastically. Consequently, the way to properly stack these shared transparencies and acknowledges the discovered secret image square measure the foremost problems. The various color visual cryptography schemes square measure. Most color visual cryptography schemes planned needed few computations. Recently, additional and additional applications of visual cryptography, like authentication, human identification, copyright protection, watermarking, mobile price tag validation, visual signature checking etc. square measure introduced.

The print and scan application of VCS are often found. During this application, scan the shares into a automatic data processing system then digitally place their corresponding shares. This may change secure verification of e-tickets or alternative documents. The developments and therefore the analysis works done by alternative researchers within the completely different views on visual cryptography, like access structure, generation of shares and alternative aspects reported by completely different authors square measure.

The visual cryptography schemes (VCS) describe the method during which a picture is encrypted and decrypted. There square measure differing kinds of visual cryptography schemes. For instance, there's the k-out-of n theme that says n shares are going to be made to cipher a picture, and k shares should be stacked to decipher the image. If the amount of shares stacked is a smaller amount than k, the initial image isn't discovered. The opposite schemes square measure 2-out-of-n and n-out-of-n VCS. The foremost of the constructions of visual cryptography schemes square measure complete using 2 n × m matrices, S0 and S1, known as basis matrices.

An effective and secure protection of sensitive information is the primary concerned in Communication systems or network storage systems. Never the less, it is also important for any information process to ensure data is not being tampered with. Encryption methods are one of the popular approaches to ensure the integrity and confidentiality of the protected information. However one of the critical vulnerabilities of encryption techniques is protecting the information from being exposed. To address these reliability problems, especially for large information content items such as secret images (satellite photos or medical images), an image secret sharing schemes (SSS) is a good alternative to remedy these types of vulnerabilities. With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been developed.

Because of the popular usage of images in network application in recent years, the way of sharing secret image has attracted wide attention. Naor and Shamir proposed first the idea of visual cryptography in 1994. The scheme provides an easy and fast decryption process that consists of xeroxing the shares onto transparencies and then stacking them to reveal the shared image for visual inspection. The scheme which differs from traditional secret sharing does not need complicated cryptographic mechanisms and computations. Instead it can be done directly by the human visual system, without the aid of computers. However the generated noisy share may be suspicious to invaders and their scheme had 2n pixel expansion at best case. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

Iwamoto and Yamamoto in 2002, worked on an n-out-of-n visual secret sharing scheme for gray-scale images. They developed a secret sharing scheme that encodes gray-scale images with a limited number of gray levels. The loss in the contrast is so large such that the recovered image is distorted. In other methods that construct a visual secret sharing scheme with a general access structure for plural secret images have been proposed .They have shown that most previous work of visual

cryptography scheme for plural image suffered from the leak out of some information in each share about the other secret images of the scheme. The systems suffered from the deterioration of the image quality in addition to the weakness in the security and there are pixels expansion step in all of method so needed some computation must be applied to reproduce the secret image.

Taking limited bandwidth and storage into consideration two criteria pixel expansion and number of shares encoded is of significance. Smaller pixel expansion results in smaller size of the share. Encoding multiple secret images into the same share images requires less overhead while sharing multiple secrets. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. To meet the demand of today's multimedia information gray and color image format should be encoded by the schemes.

Steganography is an associate degree art and a science of human action in an exceedingly means, that hides the existence of the communication. It's additionally known as an "covered writing", as a result of it uses a "cover" of a message for causation any vital secret message [3]. Steganography encompasses a long history of being used as the simplest way to shield security and privacy of valuable data. Whereas cryptography focuses on protecting the key message by jumbling its content, steganography makes attention on protecting the key message by concealing its mere existence. Using totally different techniques, we are able to send secret information within the kind of a picture, a music file or perhaps a video file by embedding it into the barer, forming a encypted signal. At the receiver's finish, the key knowledge is recovered from the stego signal with the help of totally different algorithms [3].. There are four ways that implement steganography:

1. Using text.
2. Using pictures.
3. Using audio files.
4. Using video files.

From thousands of year our ancestors are using steganography. For eg., the sender hide messages inside wax tablets, on messenger's body, on paper written in invisible inks, on envelopes lined by the stamp etc. fashionable steganography hides the key image into pictures, audio, video, text. Steganographic techniques ar classified consistent with the quilt medium used as shown within the fig below:

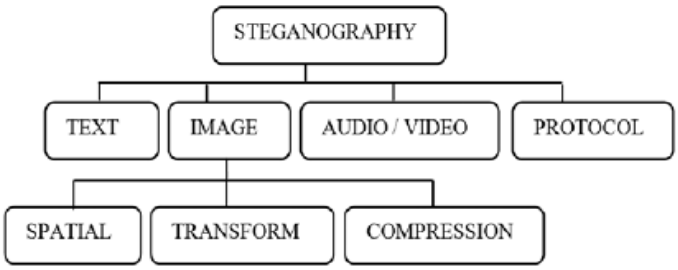

Fig 2: Classification of Steganographic Techniques

With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. One of the grounds discussed in information security is the exchange of information through the cover media. To this end, different methods such as cryptography, steganography, coding, etc have been used. The method of steganography is among the methods that have received attention in recent years [1]. The main goal of steganography is to hide information in the other cover media so that other person will not notice the presence of the information. This is a major distinction between this method and the other methods of covert exchange of information because, for example, in cryptography, the individuals notice the information by seeing the coded information but they will not be able to comprehend the information. However, in steganography, the existence of the information in the sources will not be noticed at

all. Most steganography jobs have been carried out on images, video clips,texts, music and sounds .Nowadays, using a combination of steganography and the other methods, information security has improved considerably. In addition to being used in the covert exchange of information, steganography is used in other grounds such as copyright, preventing e-document forging. Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". Steganography is the art of inconspicuously hiding data within data. The main goal of steganography is to hide information well enough such that the unintended recipients do not suspect the steganographic medium of containing hidden data Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible. Most steganography jobs have been carried out on different storage cover media like text, image, audio or video. Steganography [2] & encryption are both used to ensure data confidentiality. However the main difference between them is that with encryption anybody can see that both parties are communicating in secret. Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. This makes steganography suitable for some tasks for which encryption aren't, such as copyright marking.

Secret Communication Techniques	Confidentiality	Integrity	Un removability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes/No	Yes/No	Yes

Table 1: Comparison of secret communication techniques

This Table shows a comparison of different techniques for communicating in secret [4]. Encryption allows secure communication requiring a key to read the information. An attacker cannot remove the encryption but it is relatively easy to modify the file, making it unreadable for the intended recipient.

II. LITERATURE SURVEY

The idea of visual cryptography and secret sharing was developed by Adi Shamir. Shamir explicit that the key D is split in n range of items and simply reconstructable from any k items [1].

In 1994[1], Naor & Shamir, projected visual cryptography theme. During this, secret image is split into specifically two shares & each share is needed for the decipherment method. In this, the shares generated are purposeless and is employed for black & white pictures solely.

In 1996[2], Ateniese, Blundo & Stinson projected extended visual cryptography schemes that contain meaty share pictures. The (2,2) EVC theme projected during this needed enlargement of one picture element within the original image to four sub pixels which may then be chosen to supply the specified pictures for every share.

Until the year 1997, visual cryptography schemes were applied to solely black & white pictures. Initial colored visual cryptography theme was developed by Verheul & Tilborg[3]. The disadvantage of this theme is that they use purposeless shares to cover the key image & the standard of the recovered plain text is unhealthy.

In 2002, Nakajima & Y. Yamaguchi [4], projected a system that take a three photos as associate input & generates 2 pictures that correspond to 2 of the three input photos. The third image is recovered by stacking the 2 output pictures along.

While the previous researchers mainly concentrate on binary pictures like text pictures this paper uses the EVC theme appropriate for natural pictures like photography.

In 2003, Hou [5] projected another color VC theme, supported the halftone technique & color decomposition, it decomposes the key image into 3 colours C, M & Y. By manipulating the 3 colours values, the colour pixels within the secret image will be depicted.

In 2008, H. chu wu, Hao-cheng wang & Rui-wen yu [6], proposes a color visual cryptography theme that generate meaty shares. These meaty shares won't attract the eye of hackers. The projected theme uses the halftone technique, cowl cryptography tables & secret cryptography table to get 2 meaty shares. the key image will be recovered just by stacking the 2 meaty shares along.

In 2010, Q. Chen, X. Lv, M. Zhang, Y. Chu [7], projected associate extended visual cryptography theme with multiple secrets hidden. Meaty shares ar generated by mistreatment the principle of distinction & multiple secret pictures is also hidden by ever-changing the overlapping angle of the shares. This theme can even apply to paint image. The theme is simple & effective & shares even have spare security level.

In 2012, M. Kamath, A. Parab, A. Salyankar, S. Dholay[8], proposes a replacement visual theme for color pictures. The projected theme makes use of Jarvis error filter, a key table & specialised tables for cryptography. An encrypted binary image will be compressed with a lossless manner by finding the syndromes of low-density parity-check codes, a lossless compression technique for encrypted grey image mistreatment progressive decomposition and rate-compatible perforate turbo codes is developed in [4].

Sr. No.	Authors	Year	Image Format	Type of share generated	No. of secret Images
1.	Naor & Shamir	1994	Binary	Random	1
2.	G. Ateniese, C. Blundo, Stinson	1996	Binary	Meaningful	1
3.	E. R. Verheul & H.C.A. van Tilborg	1997	Color	Random	1
4.	M. Nakajima, Y. Yamaguchi	2002	Color	Meaningful	1
5.	Y. C. Hou	2003	Color	Meaningful	1
6.	Hsien-chu Wu, Hao-Cheng Wang & Rui-Wen Yu	2008	Color	Meaningful	1
7.	Q. Chen, X. Lv, M. Zhang, Y. Chu	2010	Color	Meaningful	Multiple
8	M. Kamath, A. Parab, A. Salyankar & S. Dholay	2012	Color	Meaningful	1

Table 2: Comparison of visual cryptography schemes on the premise of no. of secret pictures, image format

W. Liu, W. Zeng, the lossy compression technique given in [5], associate encrypted grey image will be with efficiency compressed by discarding the too rough and fine info of coefficients generated from orthogonal rework. Once having the compressed information, a receiver could reconstruct the principal content of original image by retrieving the values of coefficients. The computation of rework within the encrypted domain has conjointly been studied X. Zhang [8].

W. Liu, W. Tzeng projected, once the key information to be transmitted are encrypted, a channel supplier with none information of the science key could tend to compress the encrypted information owing to the restricted channel resource, a lossless compression technique for encrypted grey image mistreatment progressive decompose and rate compatible turbo codes is developed in [5].

The method in [6] compressed the encrypted LSBs to vacate area for added information by finding syndromes of a parity-check matrix, and therefore the facet info used at the receiver facet is that the abstraction correlation of decrypted pictures.

Fridrich et al. (2001) [3], projected the reversible information embedding technique for the authentication purpose therefore the embedding capability of this technique is low. To separate the information extraction from image decipherment, Zhang empty out house for information embedding within the plan of press encrypted pictures [4].

III. Conclusion

This paper proposed a new way for securing data in images while transmission using the combination of both steganography & visual cryptography. First of all data is hided in color image using steganographic technique then data hidden within images is kept secret using visual cryptography technique. The security of the transformation of hidden data can be obtained by using these two techniques. The combination of these two techniques can be used to increase the data security.

Acknowledgment

I would like to thank my guide for giving suggestion and guiding me in proper way.

References

1. Ms. Megha B. Goel, Mr. M. S. Chaudhari, Mrs. Shweta A. Gode “A Review on Data Hiding using Steganography & Visual Cryptography” International Journal of Engineering Development and Research (IJEDR) Volume 2, Issue 1,2014,ISSN:2321-9939
2. Mehdi Hussain and Mureed Hussain” A Survey of Image Steganography Techniques” International Journal of Advanced Science and Technology Vol. 54, May, 2013
3. Mr. Deepak S. Bhiogade, Prof. Shaikh Phiroj Chhaware” Steganography and Visual Cryptography for Secured Data Hiding” International Conference on Industrial Automation and Computing (ICIAC),13th April 2014
4. Omprasad Deshmukh 1, Shefali Sonavane “Multi-Share Crypt-Stego Authentication System” IJCSMC, Vol. 2, Issue. 2, February 2013
5. Shaveta Mahajan, Arpinder Singh” A Review of Methods and Approach for Secure Stegnography” International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE),Volume 2, Issue 10, October 2012, ISSN: 2277 128X
6. Lini Abraham, Neenu Daniel,” Secure Image Encryption Algorithms: A Review”, International Journal of Scientific & Technology Research volume 2, issue 4, April 2013, PP-186-189.
7. Mohanraj Arumugam and Rabindra Kumar Singh,“Data Hiding and Extraction Using a Novel Reversible Method for Encrypted Image” IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013, PP-1-5.
8. Kim, H.J., Sachnev, V., Shi, Y.Q., Nam, J., Choo, H.G., 2008. A novel difference expansion transform for reversible data embedding. IEEE Transaction Information Forensics and Security 3 (3), 456–465.
9. X. Zhang, “Reversible data hiding in encrypted images,” *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.
10. X. Zhang, “Separable reversible data hiding in encrypted image,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.
11. Chang, C.C., Lu, T.C., 2006” A difference expansion oriented data hiding scheme for restoring the original host images” Journal of Systems and Software 79 (12), 1754–1766.
12. W. Puech” Image Encryption and Compression for Medical Image Security” PROCEEDING OF IEEE Image Processing Theory, Tools & Applications.
13. W. Puech, M. Chaumont and O. Strauss “A Reversible Data Hiding Method for Encrypted Images” Author manuscript, published in "IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography, and Watermarking of Multimedia Contents, San Jose, CA : United States".
14. Saurabh Singh and Gaurav Agarwal,”Hiding image to video: A new approach of LSB replacement”,International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003.
15. Steganography on new generation of mobile phones with image and video processing abilities, as appeared Computational Cybernetics and Technical Informatics (ICCCCONTI), 2010 International Joint Conference on 27-29 May 2010 in Timisoara, Romania ISBN: 978-14244-7432-5.
16. Y. J. Dai., L. H. Zhang and Y. X. Yang.: A New Method of IMAGE Video Steganographying Technology. Internation –al Conference on Communication Technology Proceedings (ICCT), 2003.
17. D.-C. Wu and W.-H. Tsai: A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003.

