International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

A Review on various approaches for image steganography

Raminder jit Singh Kahlon
Research Scholar
SGGSWU
rs_kahlon01@yahoo.com

Vinay Bhardwaj
Asst. professor
SGGSWU
vinaybhardwa0708@gmail.com

Abstract- *Steganography is a technique for the secure transmission of data over the network. In this process, the secret information is transmitted by hiding this behind a signal or image or video. The Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. In this process image is divided into different regions for the detection of least significant bits available in different images. Image pixel available in the image is a combination of three different colors red, green and blue.*

Keywords*: Steganography, LSB. MLSB, RGB.*

1. INTRODUCTION

1.1 Digital Image Processing: A picture might be characterized as a two-dimensional capacity, f(x, y), where x and y are spatial (plane) coordinates, and the amplitude of at any pair of coordinates (x, y) is known as the power or gray level of the picture by then. Whenever x, y, and the adequacy values off a genuine limited, discrete amounts, we call the picture an advanced picture. The field of digital image processing alludes to preparing computerized pictures by method for an advanced PC, and known as digital image processing.

1.2 Steganography: Steganography is the craftsmanship and exploration of imperceptible communication. This is expert through concealing data in other data, subsequently concealing the presence of the imparted data. The word steganography is gotten from the Greek words "stegos" signifying "cover" and "grafia" signifying writing defining it as "covered writing".

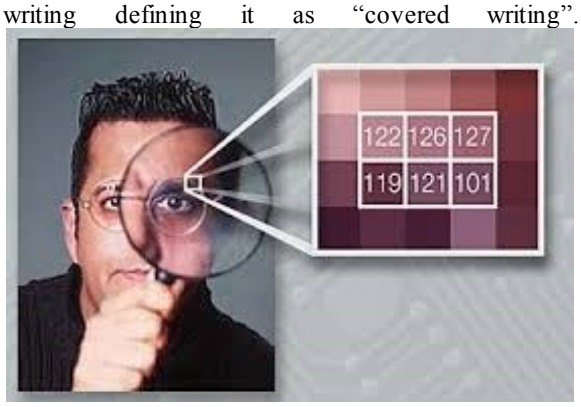


Fig. 1.1 Steganography

In image steganography the data is concealed exclusively in pictures. The benefit of steganography is that it can be utilized to covertly transmit messages without the truth of the transmission being found. Regularly, utilizing encryption may distinguish the sender or collector as some individual with something to stow away. For example, the photo of our cat could hide the arrangements for our organization's most recent specialized development.

1.3Different kind of Stenography

1.3.1 Text steganography: Hiding information in content is the most imperative strategy for steganography. The strategy was to conceal a secret message in each nth letter of each expression of an text message. In the wake of blasting of Internet and diverse sort of advanced record designs it has diminished in significance. Text stenography utilizing computerized documents is not utilized all the time on the grounds that the content records have a little measure of repetitive information.

1.3.2 Image steganography: Images are utilized as the prominent spread articles for steganography. A message is installed in a digital image through an embedding algorithm, utilizing the mystery key. The

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

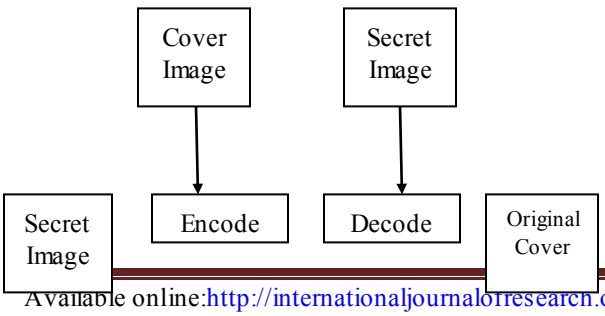
subsequent stego image is Send to the collector. On the other side, it is handled by the extraction algorithm utilizing the same key. Amid the transmission of steno picture unauthenticated persons can just notice the transmission of a picture yet can't figure the presence of the hidden message.

1.3.3 Audio steganography: Audio stenography is covering, which misuses the properties of the human ear to hide data unnoticeably. A capable of being heard, sound can be unintelligible in the presence of another louder capable of being heard sound .This property permits to choose the direct in which to hide data.

1.3.4 Protocol steganography: The term protocol steganography is to inserting data inside of system protocol, for example, TCP/IP. We hide data in the header of a TCP/IP packet in a few fields that can be either discretionary or are never utilized.

1.4 Applications of Steganography

- It can be an answer which makes it conceivable to send news and data without being controlled and without the apprehension of the messages being blocked and followed back to us.
- It is additionally conceivable to just utilize steganography to store data on an area.
- Steganography can likewise be utilized to actualize watermarking. In spite of the fact that the idea of watermarking is not as a matter of course steganography, there are a few steganography procedures that are being utilized to store watermarks in data.
- E-commerce takes into consideration an intriguing utilization of steganography. In current e-business exchanges, most clients are ensured by a username and secret key, with no genuine strategy for checking that the client is the real card holder.
- Paired with existing specialized techniques, steganography can be utilized to complete shrouded trades. Governments are keen on two sorts of shrouded interchanges: those that support national security and those that do not.



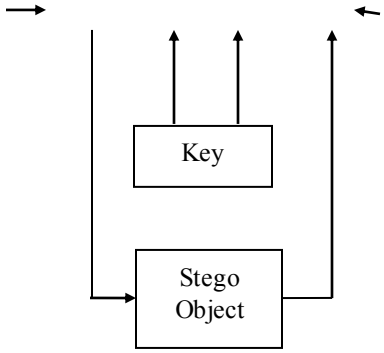


Figure 1.2: Steganography of Image

1 REVIEW OF LITERATURE

S. K. Moon et al [1] "Application of data hiding in audio-video using anti forensics technique for authentication and data security" Steganography is the method of hiding any secret information like password, text, and image, audio behind original cover file. In this paper we proposed the audio-video crypto steganography which is the combination of image steganography and audio steganography using computer forensics technique as a tool for authentication. Our aim is to hide secret information behind image and audio of video file. As video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable algorithm such as 4LSB is used for image steganography and phase coding algorithm for audio steganography. Suitable parameter of security and authentication like PSNR, histogram are obtained at receiver and transmitter side which are exactly identical, hence data security can be increased. This paper focus the idea of computer forensics technique and its use of video steganography in both investigative and security manner.

G.R.Manjula et al [2] 2015 "A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography in Spatial Domain" This paper presents a novel 2-3-3 LSB insertion method. The image steganography takes the advantage of human eye limitation. It uses color image as cover media for embedding secret message. The important quality of a steganographic system is to be less distortive while increasing the size of the secret message. In this paper a method is proposed to embed a color secret image into a color cover image. A 2-3-3 LSB insertion method has been used for image steganography. Experimental results show an improvement in the Mean squared error

(MSE) and Peak Signal to Noise Ratio (PSNR) values of the proposed technique over the base technique of hash based 3-3-2 LSB insertion.

Debiprasad Bandyopadhyay et al [3] 2014 "A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain" This paper presents a novel approach of building a secure data hiding technique in digital images. The image steganography technique takes the advantage of limited power of human visual system (HVS). It uses image as cover media for embedding secret message. The most important requirement for a steganographic algorithm is to be imperceptible while maximizing the size of the payload. In this paper a method is proposed to encrypt the secret bits of the message based on chaos theory before embedding into the cover image. A 3-3-2 LSB insertion method has been used for image steganography. Experimental results show a substantial improvement in the Peak Signal to Noise Ratio (PSNR) and Image Fidelity (IF) value of the proposed technique over the base technique of 3-3-2 LSB insertion.

Sahar A. El_Rahman et al [4] 2015 "A Comprehensive Image Steganography Tool using LSB Scheme" This paper presents a secured model for communication using image steganography. The main concern is to create a Java-based tool called IM Stego that hides information in images using Least Significant Bit (LSB) algorithm (1-LSB) and modified Least Significant one Bit algorithm, i.e. Least Significant 2 Bits algorithm (2-LSB). IM Stego is a more comprehensive security utility where it provides user-friendly functionality with interactive graphical user interface and integrated navigation capabilities. It provides the user with two operations, which are hiding secret data into images and extracting hidden data from images using 1-LSB or 2-LSB algorithm. IM Stego tool hides secrete information in color static images with formats BMP and PNG.

Omed Khalind, Benjamin Aziz et al [5] 2015 "Single-Mismatch 2LSB embedding method of steganography" This paper proposes a new method of 2LSB embedding steganography in still images. The proposed method considers a single mismatch in each 2LSB embedding between the 2LSB of the pixel value and the 2-bits of the secret message, while the 2LSB replacement overwrites the 2LSB of the image's pixel value with 2-bits of the secret message. The number of bit-changes needed for the proposed method is 0.375 bits from the 2LSBs of the cover image, and is much less than the 2LSB replacement which is 0.5 bits. It also reduces the effect of 2LSB embedding pattern of change, which results in lower probability of detection by 44% according to experimental results.

Androutsos, D et al [6] 1997 "Efficient image database filtering using color vector techniques" With the far reaching accessibility of personal computer and the amazing measure of advanced symbolism accessible, late examination has concentrated on the capacity, question and recovery of pictures from expansive picture databases. Strategies which are utilized in the blink of an eye, pre-process picture files, which are regarded to be measurable representations of picture data. Questions of shading, shape, composition, and so on., are then performed straightforwardly on these records to discover substantial pictures. The creators propose another indexing procedure which computes the multidimensional histogram of the directional subtle element in a given picture.

Behera, S.K. et al [7] "Color Guided Color Image Steganography Author utilize one part case: here we have 3 approaches to decide the bits * 3 approaches to choose the segment R, G or B. this outcomes in 9 cases. Utilizing two part case: here we have 3 approaches to decide the bits * 3 approaches to choose the segment RG, RG or GB. This outcomes in 9 cases. Utilizing three segment case: here we have 3 approaches to decide the bits * one approach to choose the segment which is RGB. This outcomes in 3 cases. The normal limit proportion is around 1/7 or 14% of the first cover media size. The mystery information is scattered all through the entire picture. Likewise, extricating the mystery information without the learning of seeds is practically unimaginable. The limit of the triple method is higher than the past procedures. By utilizing this algorithm, the proportion between the quantity of bits utilized inside a pixel to conceal part of the mystery message; and the quantity of bits in the pixels itself, which is characterized as the limit variable can be in the reach from 1/24 to 9/24 on the off chance that we utilize a most extreme of 3 bits. Also, in the event that we extend the algorithm to shroud 4 and even 5 bits the element can be expanded up to 15/24 which is above portion of the pixel bits, however the drawback is the extra commotion presented as the quantity of bits used to conceal the mystery information increment. The algorithm includes more randomization by utilizing two unique seeds produced from a client picked key keeping in mind the end goal to choose the component(s) used to conceal the mystery bits and in addition the quantity of the bits utilized inside

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

the RGB picture segment. Accordingly the hindrance of this method is its key administration.

Bailey and Curran [8] 2010 "Visual cryptographic steganography in images" Creator depicted a picture based multi-bit steganography method to build limit concealing insider facts in number of bits, i.e. Stego-1bit, Stego-2bits, Stego-3bits and Stego-4bits. Stego-1bit is the least complex of this, where it embeds the mystery message information into one MLSB (lower order bit) of the picture pixels, which is imperceptible. Hide and Seek is a sample of this strategy. Note that if this bit insertion is performed into the higher order bit (most significant bit), the estimation of the pixel will demonstrate an awesome noticeable change ruining its security. It is realized that insertion of shrouded bits into most reduced request MLSB in all shading RGB channels of the picture pixels is unnoticeable. In the Stego-2bits technique two bits of lower request MLSB in RGB picture steganography is utilized; Stego-2bits multiplied the limit of message covering up with insignificant security lessening. The limit can be improved more as in Stego-3bits and significantly more in stego-4bits, which are imperiling security as needs be. Shortcoming of this method is that the hidden bits are just uncovered as a result of the sequential storage of data.

2 APPROACHES USED

Least Significant Bit (LSB): The Least Significant Bit (LSB) is one of the primary systems in spatial space image steganography. In this workman new method of LSB steganography has been proposed which is an extemporized form of one piece LSB procedure. In the LSB approach, the fundamental thought is to supplant the Least Significant Bits (LSB) of the spread picture with the Bits of the messages to be covered up without devastating the property of the spread picture altogether. The LSB-based system is the most difficult one as it is hard to separate between the spread article and stego-object if few LSB bits of the spread item are supplanted. The minimum huge piece of a few or the greater part of the bytes inside a picture is changed to a touch of the mystery message. Computerized pictures are primarily of two sorts 24 bit pictures and 8 bit pictures. In 24 bit pictures we can install three bits of data in every pixel, one in each LSB position of the three eight piece values. Changing so as to expand or diminishing the worth the LSB does not change the presence of the picture; much so the resultant stego image looks verging on same as the spread picture.

$$\sum_{n=1}^{\infty} lsb(n)\frac{x^n}{1-x^n} = \frac{\ln(1-x^2)+\varphi_{x^2}(\frac{1}{2})}{\ln(x^2)}$$

Modified Least Signified Bit (MLSB): Secret data is covered up into the spread picture by MLSB strategy to accomplish more limit and better quality and in the edged territories the MF&PVD technique is utilized. In the MLSB strategy first mystery information is covered up into every piece of picture by standard k-LSB (k/2 bits of every pixel). At that point, for development of stego picture quality, contrast between pixel of spread picture and pixel of stego picture is lessened by supplementing the huge bits. In the MF&PVD technique the mystery information is inserted in leftover portion estimation of every square.

$$(\sum_{As\ in\ R} X_{s,R} = W_c \wedge \sum_{As\ in\ R}(max_{As}(Y_{s,R})) = H_c)$$

RGB intensity based variable: In this paper, we indicate another algorithm for RGB picture based steganography. Our algorithm exhibits the thought of securing variable number of bits in each channel (R, G or B) of pixel in perspective of the genuine shading estimations of that pixel: lower shading section stores higher number of bits. Our algorithm offers high breaking point for spread media diverged from other existing calculation. We show trial results exhibiting the transcendence of our algorithm. We similarly give close results other near algorithm in picture based steganography.

Random Algorithm: The random algorithm has turned into an answer for the less secure strategies such as successive encoding and basic LSB in video pictures. In this random algorithm, the sender and the beneficiary of the spread video subtly share a stego-key that is utilized as the seed for a pseudo-random number generator. This makes a grouping which is utilized as the file to have admittance to the RGB pixel estimations of the cover video picture. The message bit is inserted in the pixel of the spread picture as the list given by the pseudo-irregular number generator utilizing an encryption key. The two principle components of the pseudo-arbitrary

stage strategies are the utilization of watchword to have entry to the message, and the well-spread message bits over the spread video picture. This capacity decides the message sort, gets ready header data to be utilized as a part of the unraveling stage, and haphazardly encodes the message inside of the pixel estimations of the spread picture. This capacity first decides the message sort and length and encodes this as header data. At that point the capacity utilizes the random permutation function to haphazardly select pixel areas to encode the message inside. To do this the capacity decides the measurements of the spread picture, duplicates the measurements together to give the quantity of pixels accessible and arbitrarily permutate a rundown that incorporates values from 1 to the aggregate pixel values accessible in an anticipated and repeatable path by utilizing the same arbitrary seed key worth. The capacity then uses the arbitrary stage rundown to encode the message values in the spread picture. This capacity is quicker than the successive encoding on the grounds that the pixel areas are pre-computed as opposed to encoded utilizing counters and more secure in light of the fact that the message is encoded over the whole picture rather than the left divide of the picture.

$$\prod_{i=1}^{m} \Pr(C_i \neq C) = \prod_{i=1}^{m} (1 - \Pr(C_i = C))$$

4. CONCLUSION

Steganography is a system for the protected transmission of information over the network. In this procedure, the mystery data is transmitted by concealing this behind a sign or picture or video. The Least Significant Bit inserting procedure recommends that information can be covered up at all critical bits of the spread picture and the human eye would be notable notification the concealed picture in the spread record. Picture pixel accessible in the picture is a mix of three distinct hues red, green and blue. In the proposed work, the changed minimum huge piece is executed. Adjustments over customary LSB technique are acquainted with expansion the measure of information that can be hided in the spread picture. Furthermore, to build information assurance our calculation has an implicit encryption method. As LSB the yield picture of algorithm will appear to be indistinguishable to the spread picture.

REFRENCES

[1] S. K. Moon "Application of data hiding in audio-video using anti forensics technique for authentication and data security" Advance Computing Conference (IACC), 2014, pp 1110 – 1115.

[2] G.R.Manjula "A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography in Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM), 2015, pp 11-15.

[3] Debiprasad Bandyopadhyay "A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM), 2014, pp 11-22.

[4] Sahar A. El_Rahman "A Comprehensive Image Steganography Tool using LSB Scheme", I.J. Image, Graphics and Signal Processing, 2015, 10-18.

[5] Omed Khalind, Benjamin Aziz "Single-Mismatch 2LSB embedding method of steganography", IEEE Conf. on 2LSB, 2015, PP 44-54.

[6] Androutsos, Plataniotis, K.N. Venetsanopoulos, A.N. "Efficient image database filtering using colour vector techniques", IEEE Conf. on Electrical and Computer Engineering, 1997, pp 827 - 830 vol.2.

[7] Behera, S.K., Rohith, J. ; Mukund, V. ; Honwade, R. "Colour Guided Colour Image Steganography", Universal Journal of Computer Science and Engineering Technology, Vol. 1, No. 1, pp. 16-23, IEEE, 2010.

[8] Bailey, K, Chen, L.-H. "An evaluation of image based steganography methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88,IEEE,2006.

[9] Chapman, M. Davida G, and Rennhard M. "A Practical and Effective Approach to Large Scale Automated Linguistic Steganography" IEEE, Vol. 30, No.2, pp. 67-75, 2011

[10] Gutub, A., Kurinji, R. "Pixel Indicator High Capacity Technique for RGB Image Based Steganography", WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E., pp. 154-159,IEEE,2008.

[11] Gutub, A., Verma, K. ; Sahoo, A. "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, Vol. 2, No.1, pp. 193-198,IEEE,2010.

[12] Liberda, O, Bartusek, K. ; Smekal, Z. ; Mikulka, J. "Data processing in studying the temporomandibular joint, using MR imaging and sonographic techniques", IEEE conf. on Digital Signal Processing, 2009, pp 1 – 6.
[13] Marwaha, P., Marwaha, P. "Visual cryptographic steganography in images", Second International conference on Computing, Communication and Networking Technologies, pp. 34-39, IEEE, 2010.