DATA HIDING IN DIGITAL IMAGE: HISTORICAL AND CURRENT PROSPECTIVE

[1]Sangeeta, [2]Kamaldeep joshi, [3] Harkesh sehrawat, [4] Gaurav
[1]M.TECH Student, [2]Assistant Professor,[3]Assistant Professor,[4]Assistant Professor
University Institute of Engineering and Technology, Maharashi Dayanand University, Rohtak, India,
[4]Department of Computer Science & Engineering, School of Engineering Sciences & Technology, Jamia Hamdard, New Delhi, India

Abstract—Steganography is the art that added, imparting mystery information in a proper medium transporter, e.g., picture, sound, and video files. It goes under the suspicion that if the element is noticeable, the intension of the assault is obvious; accordingly the motive is dependable to cover the very presence of the original information. Be that as it may, similar to some other science it can be utilized for sick expectations. In the steganography, information conceals in terms that cannot change the secret information. It's mainly purpose is transferred data from one location to another location. It means concealed a secret data inside the other data in a manner that a critic cannot find the existence of real subject matters. Concealing the secret data in the images, various types of methods are used in which some are stronger than others to conceal the data. Steganography's definitive targets, which are imperceptibility, vigor (protection from different picture preparing strategies and pressure) and limit of the concealed information are the primary factors that differentiate it from related procedures, for example, watermarking and cryptography. This paper exhibited an overview of the real calculations of steganography conveyed in advanced imaging. The rising strategies, for example, DCT, DWT and versatile steganography are not very inclined to assaults, particularly when the concealed message is less. Steganography necessity is that the cover picture must be precisely chosen. A natural picture ought not to be utilized, it is better for stenographer to make their own particular pictures. There is some method of image steganography are discussed and these methods are different strong and weak points. In this paper, an overview is given of image steganography and its method.

Keywords—steganography, interpolation, image security, data hiding

I. INTRODUCTION

Steganography is mainly used to conceal the data in other data [1]. Steganography is derived from the Greek language "stages" means "cover" and "grafia" means" writing" use as "covered writing. Steganography and cryptography, both the techniques used to protect the data from attackers. If the secret message detects then this technology becomes a failure. Effectiveness of Steganography gains by combining it with cryptography [2].

Ancient steganography

Steganography is being used over a long time to exchange secret information from one place to another in many forms. There are some examples defined below which used the steganography. Firstly, it was used in Greece in which they choose a slave among trusted slaves and that selected slave's head was shaved and then message was written on the slave's head. And they waited until the hair was grown. After that they sent him where the message sent. The receiver removed the hairs and read the message [3]. In the same time period a warning message was sent by the Demerstus, who wrote a message to the Spartans. To send this message he was using the wax tablet that was made from the wood. And after that it was covered by the fresh wax. It seemed like an empty tablet and the secret message successfully sent [4]. During World War 2 a new technique was used to hide the information. They used the invisible ink on a paper that looked like a normal paper and sent the message. They used two different types of liquids to reveal the message and that liquid may be fruit juice or any other types of vegetables and vinegar. And at the receiver side, they used the liquid in that paper and that wet paper was heated and it became dark and the hidden message was gotten [5]. And other types of steganography were used during World War 2 that used the microdots. That dotes used for hiding the secret message [6].

Digital steganography today

In the recent days, many digital documents are used in the internet. In the internet data is not safe today's. For security purposed many researchers discovered the different types of stenographic methods that are highly secured the documents from the attackers. Therefore, to analysis the stago images there are many types of stegano-analysis software [7].Different types of mathematical equations are used in the cryptography, but it has some limitations and these are easy to crack with little efforts.

Steganography exploits an image format

Today's time secret message used over the World Wide Web is feasible through various techniques. High confidential data are transferred very easily. Steganography exploits an image format. It is done by using OS window prompt.

D: b> COPY / B dog. JPEG + secret data .txt s. JPEG

In above a secret message is appended that is found in the "secret message.txt" into the JPEG image file "dog. JPEG" and produces the stego-image "s. JPEG". When the image is opened in notepad secret data is disclosed itself. When the stego-picture is opened using the notepad, then it revealed the message after showing some information as shown in figure 1. But unluckily this method cannot prevent the addition of any types of data.

Original imagestego-image

Original message –steganography, mainly work is to hide the secret message in different formats like image, text and audio.

Figure 1 the mystery data are apparent when the stego-picture is opened using Notepad

II. STEGANOGRAPHY TYPES

There are four types.

- Text
- Audio/video
- Image
- Protocol

Spatial domain technique

Steganography in images are classified into two categories: Spatial-domain based Steganography and the Transform domain based Steganography [8]. In the spatial domain, the hidden messages are inserted specifically [8, 9]. In this, the most widely recognized and easiest Steganography technique is the least significant bits (LSB) addition strategy. In the LSB method, the pixels are supplanted by the message bits which are permuted before implanting.

LSB steganography

The LSB is the simplest method for hiding the data and widely used. In this method the secret data is hidden by changing only the last significant bit of the original image. And that's why there is no effect on the quality of the image. And the concealing capacity of the data can be increased up to last four significant bits [10]. But by the stego -analysis, it is easily detected and there from time to time there are many modifications and changing to strengthen the technique.

For example, 3 pixel grid for of a 24-bit image can be as follows:

(00101101 00011100 11011101)
(10100111 11000101 00001101)
(11010010 10101101 01100011)

When the number 500, which binary representation is11110100, is embedded into the least significant bits the result as follows:

(0010110 00011101 11011101)
(10100111 11000100 00001101)
(11010011 10101100 01100011)

Luo W et al. proposed the LSB matching approach; in that approach if the secret bit does not match with the LSB of original image than orderly manner add +1 or -1 in the pixel [11]. In Cyclic LSB we disseminate the message in the entire host picture, utilize stego shading cycle strategy for cover image. By this technique, overcome the asymmetry occurred by the simple LSB method. And this approach is not easily detected by the steganalysis. To find the M-LSB secret data there are many stegnoanylsis methods are proposed.

Mielikainen j proposed the LSB matching revisited [12]. By this technique he solved the problem occurred in the LSB-M. It is improved version of the LSB-M technique. In this technique two secret bits are added in a group of pixels. In that first secret bit is added into the first pixel and other second bit is, hidden in that pixel group that first bit is added. By this method the asymmetry occurred by the LSB method is overcome.

Bailey and Curran proposed the stego color cycle method. By this method the security of the data is increased. This technique is mainly used for the RGB images. In this technique data is concealed in different channels of the original image. This technique a cycle method is used, in that first secret bit is added in pixel 1 of the red channel and second added in the green and third added in the blue and continue till all bit is added [13]. But in this technique is problem that secret bit is added in a fixed cyclic manner and it is easily detected.

Parvez et al. proposed the pixel indicator method. In this method the RGB channels are split into three channels that are indicator and data channels. Indicator channels are used for the data, concealing that provide the security. In this technique security depends on the pixel indicator channels that are below display in table 1 [14, 15].

Table 1 Types of channels and their uses

Indicator channel	Data channel 1	Data channel2
11	Change 2 LSB bit	Change 2 LSB bit
10	Change 2 LSB bit	No bit change
01	No bit change	Change 2 LSB bit
00	No bit change	No bit change

Tsai and Wuproposed the first edge based method [16]. In these secret bits are added into the edge space pixel. All the secret bits are added into the smooth space or edge space of the image. But this method was some limitation that was easily detected by the HVS [17]. So far new approach was proposed was hybrid edge detector and by that image was not blurred and payload was also increased. Grover et al. proposed an improved version of the edge based method. In this method, in edge pixel three bits is embedded [18].

Ahmad T. Al –taani et al. proposed the hiding gray image using block method. In this method covering up of a message will decrease the likelihood of identifying the mystery message. This technique permits to shrouds dark picture in each other. In this strategy the cover is isolated into pieces of equivalent sizes; each square size is same as that size of the installing picture. [19] Contrast every pixel in installing picture and all the relating pixels in the pieces of the cover picture, i.e. pixel (i, j) in the implanting picture is contrasted and the pixel (i, j) in all C pieces of cover picture. Select the best pixel to implant.

Abdullah M. AL-Issa et al. proposed the method the gray level modification Steganography is a method to delineate (not implant or conceal it) by adjusting the gray level estimations of the picture in pixels. GLM Steganography utilizes the idea of odd and even numbers to outline inside a picture. It is a coordinated mapping between the paired information and the chose pixels in a picture. From a given picture an arrangement of pixels is chosen in light of a scientific capacity. The gray level estimations of those pixels are inspected and contrasted and the bit stream that will be mapped in the picture.

Saher manaseer proposed a new method that is standard LSB and Condition Based LSB [24]. In this method last bit of the LSB is changed in the corner to corner. This technique changes the last bit or the second minimum last bit in light of the condition as takes after: If the most significant bit is 1, the calculation changes the second minimum Significant bit. Something else, the calculation changes the last bit. This procedure is more secure contrasted with others due to relying upon the reference of information; it conceals the reference not the genuine information.

Kamaldeep joshi et al. proposed a new method for data hiding using 2-bit XOR that is dealing the picture (gray scale picture) which is 2 dimensional [25]. In this technique, vast measure of information can be concealed in light of the fact that 2 bits of information are concealed in one pixel. In that XOR activity is used in eighth bit, seventh bit, second and first bit of information. This proposed strategy likewise makes the stego picture of better quality and also gives the surety against assault.

Kamaldeep joshi et al. proposed a new LSB method that is used to inquire the PSNR and MSE of LSB information hiding procedure based on various message sizes [26]. The proposed LSB technique takes the first LSB bit of the image and first message bit of the original message and inserts the message into the first image. After adding the first message bit, pixel area of picture and message is increased by one. This procedure consistent itself till the message length isn't equivalent to zero. In this PSNR is more for the short message and less in case of long message size and MSE is less for the short message and more in case of long message size.

Transform domain technique

In this strategy, the initial step is to change the cover picture into various spaces [8]. At that point the changed coefficients are prepared to conceal the mystery data. These changed coefficients are changed over into spatial space to get stego picture. The upside of change, area strategies is the highest capacity to confront flag preparing activities. Be that as it may, techniques for this write are computationally unpredictable. Steganography strategies utilizing DCT (Discrete Cosine Transforms), DWT, DFT (Discrete Fourier Transforms) go under this class.

DWT (Discrete Wavelet Transform)

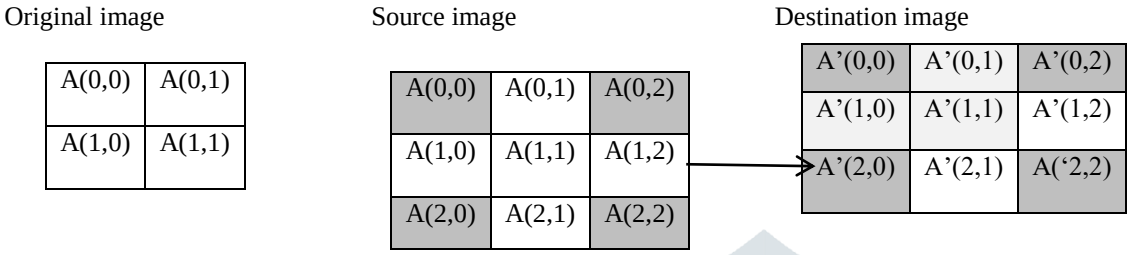
The DWT separates a picture into four sections to be specific a lower determination estimate segment (LL) and also the horizontal level (HL), vertical (LH) and slanting (HH) detail parts. The LL sub band is gotten after low-pass separating both the lines and sections and contains a harsh portrayal of the picture. The HH sub-band is high-pass separated in the two bearings also, have the high-recurrence parts along the diagonals.

Provos et al. proposed the OutGuess method that was a superior option as it utilized a pseudo-arbitrary number generator to choose DCT coefficients [20]. The X2-test does not identify information that is arbitrarily disseminated. The designer of OutGuess recommends a counter-assault against his calculation. They recommend applying a broadened form of the X2-test to choose Pseudo-arbitrarily implanted messages in JPEG pictures.

Abdelwahab and Hassan proposed a discrete wavelength transformed technique [21]. In this method information, concealing procedure used in the DWT space. Both mystery and cover pictures are disintegrated utilizing DWT (first level). Each of which is partitioned into disjoint 4 squares. Pieces of the mystery picture fit into the cover squares to decide the best match. Thereafter, blunder squares are created and implanted into coefficients of the best coordinated pieces in the HL (horizontal level) of the cover picture. Two keys must be imparted; one holds the records to the coordinated squares and another for the coordinated pieces in the CHL (central horizontal level) of the cover. Note that the separated payload isn't absolutely indistinguishable to the implanted form as the main inserted and removed bits have a place with the mystery picture guess while setting every one of the information in other sub-pictures to zeros amid the remaking procedure.

Thomas Lehmann et al. proposed the interpolation method [22]. In this nearest neighbor method are used and only nearest point values are selected and other values are discarded. By the closest neighbor technique, one can find the nearest relating pixel in the source picture p (I, J) for every pixel in the goal picture pixel p′ (I, J). Closest neighbor addition experiences typically unsuitable associating impacts as to developing and decreasing pictures. This technique produces a picture that has a smoother appearance that closest neighbor. By this method image was blurred so it was not effective.

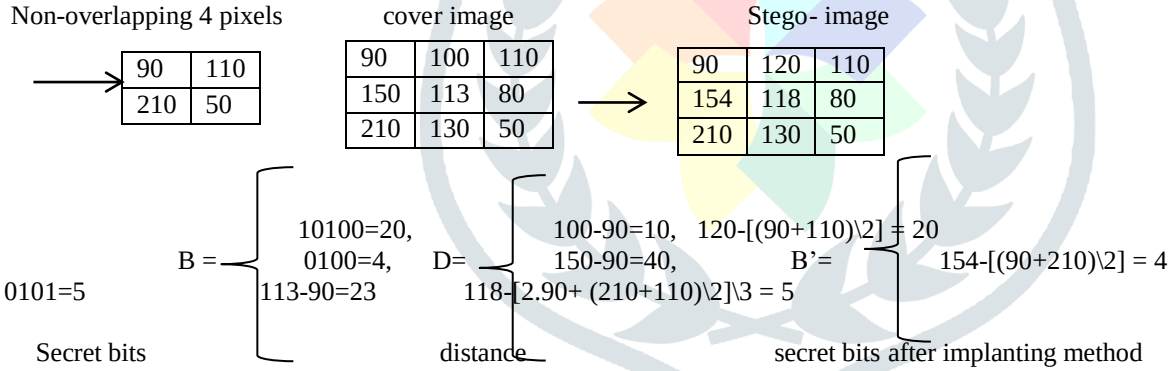
Jung and Yoo proposed the new method for interpolation that is the Neighbor means interpolation method [23].This method is used to calculate mean from the neighboring pixel values and after calculating the mean values, then inserted into the pixel that has not allotted that are displayed below in figure 2 and figure 3. Figure 2 demonstrates to a case the neighbor mean. The resulting picture is scaled two times more. On account of i<j, A′(0,1) is ascertained from (a(0,0) + a(0,2))/2 task. Whenever i<j, A′(1,0), is the aftereffect of (a(0,0) + a(2,0))/2. At long last, A′(1,1) is gotten from (a(0,0) + a′(0,1) + a′(1,0))/3.



A’ (0, 1) = (a (0, 0) + a (0, 2))/2
A’ (1, 0) = (a (0, 0) + a (2, 0))/2
A’ (1, 1) = (a (0, 0) + a’ (0, 1) + a’ (1, 0))/3

Figure 2: Construction of four pixels, non-overlapping consecutive blocks in a cover image

For example,a(0,1) is calculated by(a′(0,0) + a′(0,2))/2=(90+110)/2=120 and the secret data embedding in a(0,1) is 120− 100=20. A(1,0) is additionally ascertained by (a′(0,0) + a′(2,0))/2=(90 + 210)/2=154 and the mystery information implanting in p(1,0) is 154 − 150=4. Finally, a(1,1)is obtained by(a′(0,0)+a′(0,2)/2+a′(2,0)/2)/3=(2.90+(210+110)\2)\3)=5,and secret data embedding in A′(1,1) are118− 113=5.This means that the cover image and secret data can be extracted by utilizing stego-picture as it were. Below Bis used as a secret bit, D is the distance between two pixels and B’ is used as after interpolation getting secret values. Secret bits (B) are 1010001000101 used.



III. EVALUATION

There is some method of image steganography are discussed and these methods are different strong and weak points. Below Table 2 are used to analysis the strong or weak points of different techniques

Table 2 Analysis the strong or weak points of different techniques

Technique	**Comparison**		
	Technique	***Proposed by***	***Conclusion***
1	LSB matching approach	Luo W et al.	It is improved version of the LSB and some stegno-analysis is detected and is not secure.
2	LSB matching revisited	Mielikainen j	It reduces the asymmetry caused by the LSB and detection is difficult.
3	LSB stego color cycle method	Bailey and Curran	It uses the fixed cycle and by applying stego analysis is easily detected.
4	Pixel indicator method	Parvez et al.	In this method indicator channel are used if they detected, then security is no longer secure the secret data.
5	Edge based method	Tsai and Wu	This data is placed in the edge space and by this it is easily detected because the image is distorted by using this technique
6	Hiding gray image using block method	Ahmad T. Al –taani et al.	In this secret data is stored in blocks by using RGB colors.

Technique	Comparison		
	Technique	***Proposed by***	***Conclusion***
7	The gray level modification Steganography	Abdullah M. AL-Issa et al.	It is modified version of the gray level method. And it uses the odd even sequence to hide the data.
8	The OutGuess method	Provos et al.	The pseudo random number generator used to hide the data and it is providing the less security.
9	Discrete wavelength transformed technique	Abdelwahab and Hassan	In that image is divided into blocks 4*4 and error blocks are used to hide the data.
10	The interpolation method	Thomas Lehmann et al.	In this image scale up and divided into four parts and nearest neighbor values are used, but simply it is easily detected by attackers.
11	Neighbor mean interpolation method	Jung and Yoo	It is improved version of the interpolation method and used the neighbor mean method and it is high Secured as compare above.
12	Standard LSB and Condition Based LSB	Saher manaseer	This procedure is more secure contrasted with others due to relying upon the reference of information; it conceals the reference not the genuine information.
13	An Enhanced Method for Data Hiding using 2-Bit XOR	kamaldeep joshi et al.	In this technique, vast measure of information can be concealed in light of the fact that 2 bits of information are concealed in one pixel. This proposed strategy likewise makes the stego-picture of better quality and also gives the surety against assault.
14	PSNR and MSE based investigation of the LSB	kamaldeep joshi et al.	In this PSNR is more for the short message and less in case of long message size and MSE is less for the short message and more in case of long message size.

IV. CONCLUSION

This paper exhibited an overview of the real calculations of steganography conveyed in advanced imaging. The rising strategies, for example, DCT, DWT and versatile steganography are not very inclined to assaults, particularly when the concealed message is less. Steganography necessity is that the cover picture must be precisely chosen. A natural picture ought not to be utilized, it is better for stenographer to make their own particular pictures. There is some method of image steganography are discussed and these methods are different strong and weak points. If anyone decides which algorithm to use then firstly he decides which application he wants to use for any particular algorithm. In this we find that some algorithms are able to hide the original message, but they don't provide security. So there are some changes invented that any detector cannot intercept the data. There is some method of image steganography are discussed and these methods are different strong and weak points. In this paper, an overview is given of image steganography and its method.

REFERENCES

[1] G.G F. A. P. Petitcolas, F. A. P. Anderson, and M. G. Kuhn, "Information Hiding- A Survey", Proceedings of the IEEE, Volume 87, Issue 7, pp. 1062-1078, 1999.

[2] M. E. Saleh, A. A. Aly and F. A. Omara, "Data Security Using Cryptography and Steganography Techniques", International Journal of Advanced Computer Science and Applications, Volume7, Issue 6, 2016.

[3] Shirali-Shahreza and M. Shirali-Shahreza, "Steganography in Textiles", 4th International Conference on Information Assurance and Security", Volume 3, Issue 6, pp. 5661, 2008.

[4] K. M. Singh, L. S. Singh, A. B. Singh and K. S. Devi, "Hiding Secret Message in Edges of the Image", International Conference on Information and Communication Technology, Volume 5, Issue 1, pp. 238-241, 2007.

[5] Rahate, N. D. Rothe and P. R., Rothe, "Data Hiding Technique for Security by using Image Steganography", International Conference on Industrial Automation and Computing , Volume 8, Issue 7, pp. 33-36, 2014.

[6] J. Caldwell, "Steganography using the technique of orderly changing pixel component", International Journal of Computer Applications, Volume 58, Issue 6, 2014.

[7] N. Provos, & P. Honeyman, "Hide and Seek: An introduction to steganography", Security and Privacy, Volume 1, Issue 3, pp. 32-44, 2003.

[8] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: survey and analysis of current methods", Signal Processing, Volume 90,Issue 3, pp. 727-752, 2010.

[9] Kamaldeep, "Image steganography techniques in spatial domain, their parameters and analytical techniques: a review article", International Journal, Agriculture, Innovations, Research , Volume 2, Issue 5, pp. 85-92, 2013.

[10] R. Wang, C. Lin, J. Lin, "Hiding data in images by optimal moderately significant-bit replacement", IEE Electron., Volume 36, Issue 25, pp. 2069–2070, 2000.

[11] W. Luo, F. Huang, J. Huang, "Edge adaptive image steganography based on LSB matching revisited", Inform Forensic Secure, Volume 5, Issue 7,pp. 201–214, 2010.

[12] J. Mielikainen, "LSB is matching revisited", Signal Processing, IEEE, Volume 13, Issue 5, pp. 285–287, 2006.

[13] K. Bailey, and K. Curran, "An evaluation of image based steganography methods", Multimedia Tools, Volume 2, Issue 2, pp. 55–88, 2006.

[14] M. T. Parvez and A. Gutub, "Vibrant color image steganography using channel differences and secret data distribution". Kuwait J Science Eng., Volume 38, Issue 28, pp. 127–142, 2011.
[15] M. T. Parvez and A. Gutub, "RGB intensity based variable-bits image steganography", In: Asia-Pacific Services Computing Conference IEEE., Volume 8,Issue 33, pp. 1322–1327, 2008.
[16] S.Dumitrescu, Wu X, Wang Z, "Detection of LSB steganography via sample pair analysis", Signal Process, IEEE Trans, Volume 51, Issue 7, pp. 1995–2007, 2003.
[17] W-J Chen, C-C Chang, Le T, "High payload steganography mechanism using hybrid edge detector", Expert System Application, Volume 37,Issue 4, pp. 3292–3301, 2010.
[18] N. Grover, A. Mohapatra, "Digital Image authentication model based on edge Adaptive Steganography" In: Advanced Computing, Networking and Security, 2nd International Conference, Volume 34, Issue 2, pp. 238–242, 2013.
[19] A. T. Al-Taani, A. M. Al-Issa "A novel Steganographic method for gray-level images", Int J Computer Inform System Science and Engineering, Volume 3, Issue 1, 2009.
[20] N. Provos, P. Honeyman, Hide and seek, "An introduction to steganography", IEEE Security and Privacy, Volume 1, Issue 3, pp. 32–44, 2003.
[21] A. A. Abdelwahab, L. A. Hassan, "A discrete wavelet transform based technique for image data hiding", in Proceedings of 25th National Radio Science Conference, NRSC 2008, Egypt, Volume 18–20, Issue 2, pp. 1–9, 2008.
[22] K. H. Jung and K.Y. Yoo, "Data hiding method using image interpolation", computer standard and interfaces, Volume 31, Issue 2, pp. 465-470, 2009.
[23] K. H. Jung and K. Y. Yoo, "Steganographic method based on interpolation and LSB substitution of digital images", Multimedia Tools and Applications, Volume 74, Issue 6, pp. 2143–2155, 2015.
[24] S. manaseer, A. Aljawawdehand, D. Alsoudi, "A new Image steganography depending on reference & LSB", International Journal of Applied Engineering Research ISSN 0973-4562, Volume 12, Issue 9, pp. 1950-1955, 2017.
[25] K. Joshi, R. Yadav and G. Chawla, "An Enhanced method for data hiding using 2 bit XOR in image steganography", International Journal of engineering and technology, Volume 8, Issue 6, pp. 3043-3055, 2017.
[26] K. Joshi, R. Yadav and S. Allwudia, "PSNR and MSE based investigation of LSB", Proceedings of the IEEE, International Conference on Computational Techniques in Information and Communication Technologies, 2016.