RESEARCHERID
THOMSON REUTERS

[Singh * *et al.*, 7(7): July, 2018]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW

Ankita Singh[*1] & Chandradatta Verma[2]

[*1&2]Department of Electronics and Telecommunication Engineering, SSITM, Bhilai (C.G.)

DOI: 10.5281/zenodo.1305820

ABSTRACT

Data security and data hiding are the two important area of research now a days. There are such large number of research is progressing in the field, for example, web security, steganography, cryptography. Steganography is a trail of events used to put a sheltered data in a host media with small debilitating in have and the best approach to remove the ensured data after some time. Reversible Steganography ceaselessly is a system to introduce additional message into some distortion unsatisfactory cover media, for instance, military or therapeutic images, with a reversible way so the principal cover data can be immaculately restored after extraction of the covered message. Most covering strategies perform data embedding by changing the substance of a host media. These sorts of data hiding strategies are in this way irreversible. In different areas like military, legitimate and medical imaging introduction of some mutilation is allowable, ceaseless loss of data is unwanted. These features the prerequisite for Reversible (Lossless) data embedding methodologies. This paper displays a review of various steganography techniques.

Keywords: Steganography.

I. INTRODUCTION

Nowadays, with the quick progression of information development more images and information are available on the web. Thus there is a need to give a type of affirmation to such basic information. Exactly when the sender transmits the photo to the receiver, there may be interlopers present amidst who may get the image. In the wake of getting the image, the intruder may see the critical information in the image. This may not be the issue now and again. In any case, if we consider medical and military images then such change is unsuitable.

Steganography is a Greek work which implies the secured composing. Steganography is a craft of concealing information in a secured media (image, sound, video, content). In Steganography, we shroud the negligible nearness of that it will be imperceptible. The shrouded media is picked in such a way, to the point that it has ability to conceal the information and vigor that gives quality to the stego image. As in the up and coming years the need of information concealing, copyright security, and privacy builds, steganography assumes a vital part in this field in view of its some remarkable highlights. In this paper, we center around the distinctive steganography strategies. This audit paper gives some critical information about steganography techniques that will help in future inquires about in steganography and information concealing field. This paper is partitioned into various areas in which we clarify steganography framework, related work, diverse steganography strategies and conclusion.

From the old era, Steganography is utilized to shroud the secret data. The information was covered up on the back of wax, composing tables, stomach of rabbits or on the scalp of the slaves. Also, now daily, hacking is utilized for an unapproved access of information in this way, to keep the information private, sender utilizes diverse techniques. Steganography is one of the techniques in which the information is covered up in the cover data with the utilization of secret key. The extractor ought to have the secret key to separate the information. Design of steganographic system is such a way that an unusual user cannot find secret key. In Steganography frameworks following terms are utilized:

Cover Media: The cover media is the medium in which message is implanted to conceal the nearness of mystery information.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Stego: The media through which the information is covered up

Secret information: The information to be covered up or remove.

Steganalysis: The procedure by which mystery information is to be removed.

Data hiding system expects to insert some mystery data into a carrier signal by changing the irrelevant parts for copyright security or incognito correspondence. Generally, the data hiding operation will bring about twisting in the host signal.However, such mutilation, regardless of how little it is, is inadmissible to a few applications, e.g., military or restorative pictures. For this situation it is necessary to insert the extra mystery message with a reversible way so that the first substance can be impeccably reestablished after extraction of the concealed data.A number of reversible data hiding strategies have been proposed, and they can be generally arranged into three categories: lossless compression based methods[4] difference expansion (DE)methods[5][6], and histogram modification (HM) methods[7].The lossless compression based techniques make utilization of statistical redundancy of the host media by performing lossless compression so as to make an extra space to suit extra secret data.

II. STEGANOGRAPHY MODEL

Present day steganography utilizes the chance of concealing information into advanced interactive media documents.

Hiding information into a media requires following elements[1]

- The cover media(C) that will hold the hidden data
- The secret message (M), may be plain text, cipher text or any type of data
- The stego function (Fe) and its inverse (Fe-1)
- An optional stego-key (K) or password may be used to hide and unhide the message.

The stego function works over cover media and the message (to be covered up) alongside a stego-key (alternatively) to create a stego media (S).

The schematic of steganographic activity is demonstrated as follows.

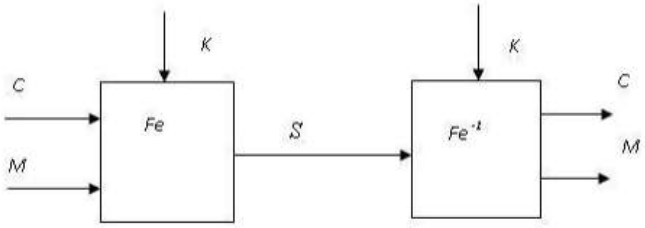

Fig 1. The Steganographic Model

III. PERFORMANCE ANALYSIS OF STEGANOGRAPHIC TECHNIQUES

Information inserting in the reversible way which is the information installing with no hardship embeds the information or payload into cutting edge picture in reversible way. After information inserting the idea of one of a kind picture may be ruined which is to be kept up a vital separation from. The charming property of information installing in reversible way is reversibility, which is after information extraction the main quality picture is restored back. Reversible information covering up hides a few information in a propelled picture in a way that an embraced party picture to its one of a kind state. The introduction of a reversible information inserting computation can be estimated using following,

- Data implanting Capacity constrain
- Visual quality
- Complexity

The information with no bowing implanting is the engaging component of reversible information stowing away. Information will emphatically change the principal substance by inserting a couple of information into it. To be

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

sure, even an extraordinarily slight change in pixel characteristics may not if its all the same to you particularly in military information and remedial information. In such conditions, every little bit of information is fundamental. From the application point of view, since the division between the implanted picture and one of a kind picture is for all intents and purposes perceivable from human eyes, reversible information installing could be thought as a best secret correspondence channel since reversible information inserting can be used as an information transporter.

IV. BASIC STEGANOGRAPHY METHODS

The reversible data covering up was done utilizing reversible data concealing calculations. A lot of research on reversible data hiding has been done in the course of recent years. Some vital systems are talked about here. Different methods have been proposed and research has been done in the field of reversible data hiding. Likewise numerous propelled strategies have been presented for reversible data hiding and visual cryptography. Some methods that are used for reversible data hiding are illustrated below:

A. Spatial Domain Methods

Steganography techniques that modify the cover image and the secret image in the spatial domain are known as spatial domain methods. It involves encoding at the LSBs level.

Least Significant Bit Substitution (LSB) [31] is the most comm only used stenographic technique. The basic concept of Least Significant Bit Substitution includes the embedding of the secret data at the bits which having minimum weighting so that it will not affect the value of original pixel.

A new steganographic method to hide a secret message into a gray -valued cover image was proposed [32]. For embedding a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. In each block, a difference value is calculated from the values of the two pixels. Then that difference value is replaced by a new value to embed the value of the secret message. This method produces a more imperceptible result than those obtained from simple least-significant-bit substitution methods. The embedded secret message can be extracted from the resulting stego-image without referencing the original cover image.

Iuon-Chang Lin [33] proposed a Data hiding scheme with distortion tolerance which uses spatial domain for hiding data. This method provides distortion tolerance and gives better quality of processed image. This scheme provides effective results than other schemes in terms of distortion tolerance.

As LSB insertion is simpler and good for steganography, we can try to improve one of its major drawbacks: the ease of extraction. We don't want that an eavesdropper be able to read everything we are sending.

B. Frequency Domain Methods

The requirement for improved security, has prompted the advancement of different calculations. LSB strategy has frail protection from assaults. So to defeat this inadequacy, specialists found a superior route for concealing information in zones of the image that are less presented to pressure, trimming, and image handling.

A lossless and reversible steganography plot has been presented that utilization each square of quantized discrete cosine transformation (DCT) coefficients in JPEG images for implanting mystery information [6]. In this plan, the two progressive zero coefficients of the medium frequency parts in each square are utilized to shroud the mystery information. This strategy brings about a high image nature of stego image and effectively accomplishes reversibility.

A reversible information concealing plan that utilization the histogram moving strategy in light of DCT coefficients was proposed [8]. Cover images are apportioned into a few unique frequencies, and the high-frequency parts are utilized for inserting the mystery information. For concealing mystery information, this technique for histogram moving movements the positive coefficients around zero to one side and the negative coefficients around zero to the lef . It enhances the concealing limit and nature of the stego-images. On switching the frequency domain stego-image back to the spatial domain image may cause undercurrent and flood issues.

Wavelets transform (WT) changes over spatial domain information to the frequency domain information. Wavelets are utilized as a part of the image steganographic demonstrate in light of the fact that the wavelet transform unmistakably parcels the high frequency and low-frequency information on a pixel by pixel premise.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Numerous down to earth tests propose to utilize the Wavelet transform domain for steganography in view of various focal points. The utilization of such transform will for the most part address the limit and heartiness of the Information Hiding framework highlights.

A Haar discrete wavelet transformation (HDWT)- based reversible information concealing technique was proposed in 2009 [9]. In this strategy a spatial domain image is transformed into a HDWT-based frequency domain image and after that the high frequency coefficients are utilized to insert the mystery information. This strategy gives a high concealing limit and a decent stego-image quality.

In the ongoing year DWT based calculation for image information stowing away has been suggested that utilizations CH band of cover image for concealing the mystery message. Vijay kumar [10] proposed a calculation in which mystery message is insert in various groups of cover image. PSNR has been utilized to gauge the nature of stegano image and it gives better PSNR by supplanting blunder obstruct with askew detail coefficients (CD) as contrast with different coefficients.

Another image steganography procedure in light of Integer Wavelet Transform (IWT) and Munkres' task calculation was presented [11]. IWT changes over spatial domain information to the frequency domain information. For inserting mystery information, task calculation is utilized for best coordinating between squares. Stego image is subjected to different kinds of image handling assaults and it demonstrates high strength against these assaults.

Prabakaran G. [12] proposed a steganography approach for concealing an extensive size mystery image into a little size cover image. Arnold transformation is performed to scrambles the mystery image. Both mystery and cover images are disintegrated utilizing discrete wavelet transform (DWT) and took after by Alpha mixing task. Discrete wavelet coefficients are utilized for concealing the information keeping in mind the end goal to boost the concealing limit. This DWT based approach gives high security and certain robustness.

C. Adaptive Methods

Versatile steganography is an exceptional instance of the spatial and transform systems. Additionally, it is presented as insights mindful implanting and covering. Worldwide measurable qualities of the image are essentially utilized before any endeavor to manage its frequency transformed coefficients. These insights choose what changes can be made. An irregular versatile choice of pixels really describes this technique, depending on the cover image and the choice of pixels in a square with an extensive standard deviation (STD). The last is expected to maintain a strategic distance from regions of uniform shading, for example, smooth territories. This method is known for abusing images with existing or intentionally included commotion and with images that show shading multifaceted nature [13-16].

A versatile least-significant bit (LSB) steganographic strategy was proposed [17]. This technique incorporates pixel value differencing (PVD) which utilizes the distinction value of two sequential pixels to gauge what number of mystery bits will be implanted into the two pixels. The PVD approach is utilized to separate the smooth and edge zones. A k-bit LSB substitution strategy is utilized for concealing information in the pixels situated in the edge regions. The scope of distinction values is adaptively separated into three unique levels that are bring down level, center level, and more elevated amount. This technique brings about bigger payload limit and high image quality.

Another strategy which makes utilization of additionally encompassing pixels around an objective pixel to locate the most suitable limit value with a specific end goal to enhance intangibility was presented [18]. As contrast with other steganographic systems which utilize either three or four nearby pixels around an objective pixel, this procedure can use each of the eight contiguous neighbors, which enhances the intangibility value.

V. CONCLUSION

This paper looked into the fundamental steganographic systems. Every one of these procedures endeavors to fulfill the three most essential variables of steganographic plan (impalpability or imperceptibility, limit, and strength). LSB systems in a spatial domain have a high payload limit, yet they regularly neglect to anticipate measurable assaults and are in this way effortlessly distinguished.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

The promising strategies, for example, DCT, DWT and the versatile steganography are not inclined to assaults, particularly when the shrouded message is little. They change the coefficients in the transform domain, in this way brings about least image contortion. By and large, such procedures have a tendency to have a lower payload when they are contrasted with the spatial domain calculations. The investigations on the discrete cosine transform (DCT) coefficients have presented some encouraging outcomes and afterward they have redirected the specialists' consideration towards JPEG images.

The current framework contains a few weaknesses so the future extension is to evacuate the inconveniences by including reversible way implies, data extraction and recuperation of picture are free of blunders. The PSNR will be enhanced to get unique cover back. In future it might conceivable that memory space can be saved before encryption which requires less measure of time for data extraction and picture recuperation.

REFERENCES

[1] Steganographic Techniques and their use in an Open-Systems EnvironmentBret Dunbar, The Information Security Reading Room, SANS Institute 2002.
[2] W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.
[3] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding, In Proc. of International Symposium on Circuits and Systems, Bangkok, Thailand, Vol. 2, pp. 912-915, 25-28 May 2003.
[4] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.
[5] J. Tian, "Reversible data embedding using a difference expansion,"IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[6] J. Tian, "Reversible Watermarking by Difference Expansion", In Proc. of Workshop on Multimedia and Security, pp. 19-22, December 2002.
[7] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129–1143, 2009.
[8] Yih-Kai Lin, "High capacity reversible data hiding scheme based upon discrete cosine Transformation", The Journal of Systems and Software 85 (2012) 2395– 2404.
[9] Y.-K. Chan et al, "A HDWT-based reversible data hiding method", The Journal of Systems and Software 82 (2009) 411– 421.
[10] Vijay Kumar and Dinesh Kumar, "Performance Evaluation of DWT Based Image Steganography", 2010 IEEE 2nd International Advance Computing Conference.
[11] N.Raftari, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", 2012 Sixth Asia Modelling Symposium.
[12] Prabakaran. G and Bhavani.R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].
[13] E. Franz and A. Schneidewind., "Adaptive steganography based on dithering", in Proc. Of the 2004 workshop on Multimedia and Security, 2004. pp. 56-62.
[14] R. Bohm and A. Westfeld, "Breaking cauchy model-based JPEG steganography with first order statistics", In Proc. of ESORICS'2004, 2004. pp. 125-140.
[15] A.M. Fard, M. Akbarzadeh-R., and F. Varasteh-A., "A new genetic algorithm approach for secure JPEG steganography", in Proc. of IEEE International Conference on Engineering of Intelligent Systems ICEIS, 2006. pp. 216-219.
[16] A. Shaddad, J. Condell, K. Curran, and P. Mckevtt.,"Biometric inspired digital image steganography", In Proc. of the 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, 2008. Pp. 159-168. [16] Yang et al., "Adaptive data hiding in edge areas of images with
[17] spatial LSB domain systems", IEEE transactions on information forensics and security, vol. 3, no. 3, september 2008.
[18] Masoud Afrakhteh and Subariah Ibrahim, "Adaptive Steganography Scheme Using More Surrounding Pixels", IEEE International Conference On Computer Design And Appliations (2010).
[19] Z.Ni, Y.Q. Shi, N. Ansari, andW. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.
[20] S. K. Lee, Y. H. Suh, and Y. S. Ho, "Reversible image authentication based on watermarking," in Proc. IEEE ICME, 2006, pp. 1321–1324.
[21] M. Fallahpour, "Reversible image data hiding based on gradient adjusted prediction,".

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[22] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[23] W. Hong, "An efficient prediction-and-shifting embedding technique for high quality reversible data hiding," EURASIP J. Adv. Signal Process., vol. 2010, 2010.
[24] D. Coltuc, "Improved embedding for prediction-based reversible watermarking," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 873–882, Sep. 2011.
[25] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
[26] W. Hong, "Adaptive reversible data hiding method based on error energy control and histogram shifting," Opt. Commun., vol. 285, no. 2, pp. 101–108, 2012.
[27] C. Wang, X. Li, and B. Yang, "High capacity reversible image watermarking based on integer transform," in Proc. IEEE ICIP, 2010, pp. 217–220.
[28] Che-Lun Pan, Wien Hong, Tung-Shou Chen, Jeanne Chen and Chih-Wei Shiu, "Multilevel Reversible Data Hiding using Modification of Prediction Errors", ICIC Vol 7,No. 9, Sept 2011.
[29] Xiaolong Li, Bin Yang and Tieyong Zeng, "Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection", IEEE Transaction on Image Processing, Vol, 20, No. 12, Dec 2011.
[30] Kuo-Ming Hung, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen, " Reversible Data Hiding Base on VQ and Halftoning Technique", International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).
[31] Chan, C.K., Chang, L.M., "Hiding data in image by simple LSB substitution", Pattern Recognition, vol 37, pp.469-471, 2003.
[32] Da-Chun Wu, Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters 24 (2003) 1613–1626.
[33] I.-C. Lin et al, "Hiding data in spatial domain images with distortion tolerance", Computer Standards & Interfaces 31 (2009) 458–464

CITE AN ARTICLE

Singh, A., & Verma, C. (2018). IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 7*(7), 18-23.