# A Review on Steganography Techniques

Rituraj Gaur[1] and Dr. Rekha Vig[2]
[1]*M.Tech Student*, [2]*Associate Professor*
*Department of Electrical, Electronics and Communication Engineering*
*The North Cap University, Gurugram, Haryana, India.*

***Abstract*** **-** Steganography can be described as the examination of intangible correspondence that as a rule deals with the techniques for disguising the nearness of the passed on message. If it is refined successfully, the message does not attract thought from meddlers and aggressors. The essential goals of steganography are impalpability, quality and utmost of the covered data. These are the key segments which make it not exactly the same as various strategies watermarking and cryptography. This paper consolidates the basic steganography strategies and the essential spotlight is on the overview of steganography in cutting edge pictures.

***Keywords*** **-** Adaptive steganography, Frequency domain, Image steganography, Spatial domain, Steganography.

## I. INTRODUCTION

In current era, web offers magnificent convenience in transmitting a great deal of information in different parts of the world. In any case, the prosperity and security of long partition correspondence remains an issue. Remembering the true objective to handle this issue has incited the headway of steganography methods.

Steganography is the science that gives secret information in a legitimate intuitive media carrier, e.g., image, sound, and video reports. Steganography isn't the same as cryptography. The key objective of cryptography is to secure correspondences by changing the information into a shape with the objective that it can't be understand by a rubberneck. On the other hand, steganography methodologies tend to cover the nearness of the message itself, which makes it troublesome for an onlooker to comprehend where correctly the message is.

There are other two movements that are enduringly identified with steganography are watermarking and fingerprinting [1]. These movements are principally worried over the security of authorized development, thusly the include have shocking basics stand out from steganography. In watermarking the greater part of the occasions of a test are "set apart" similarly. Obviously, in fingerprinting novel etchings are embedded in unmistakable duplicates of the transporter challenge that are given to various clients. This empowers the authorized development proprietor to perceive clients who break their affirming perception by giving the property to untouchables [1].For an impressive time allotment people have hidden information in different ways. Steganography is a kind of hid correspondence that really connotes "secured expressing" (from the Greek words stegano or "secured" and graphos or "to form"). In 1550, Jerome Cardan, an Italian mathematician, proposed an arrangement of secret forming where a paper cover with openings is used. The customer needs to create his secret message in such holes consequent to setting the cover over a reasonable sheet of paper. By then empty the cover to fill free parts of the page and thusly the message appears as innocuous substance [2].

The execution of a steganographic structure can be assessed using a couple of properties. The most basic property is the verifiable subtlety (vagary) of the information, which exhibits that it is so difficult to choose the nearness of a covered message. Other related measures are as far as possible, which is the best information that can safely installed in a work without having quantifiably recognizable things and generosity, which insinuates how well the steganographic structure restricts the extraction of covered information.

This paper is organized as follows. Area II rapidly analyzes the crucial idea of steganography strategy. Fragment III portrays the spatial space methodology which incorporates encoding at the LSBs level. Zone IV depicts the repeat space systems, for instance, discrete cosine change (DCT) and discrete wavelet change (DWT). Portion V delineates adaptable steganography which is a one of a kind occurrence of the spatial and changes systems. Fragment VI addresses examination of the various existing procedures for steganography, Segment VII exhibits a concise writing overview of the considerable number of works that have been done toward this path. Finally zone VIII gives the conclusion.

## II. STEGANOGRAPHY MODEL

A basic steganographic model is shown in figure 1. The process of embedding can be explained as:

Let $X$ represents the cover image, and $Z$ the stego-image. Let $K$ be a stego-key (as a seed used to encrypt the message, which can be set to □□□for simplicity), and let $M$ be the message that the sender wishes to send. Then, $E_{\blacksquare}$ represents an embedded message and $E_{\blacksquare}$ represents the extracted message. Therefore,

$$E_m : X \oplus K \oplus M \rightarrow Z$$
$$\therefore E_x\left(E_m\left(x,k,m\right)\right) \approx m, \forall x \in X, k \in K, m \in M$$

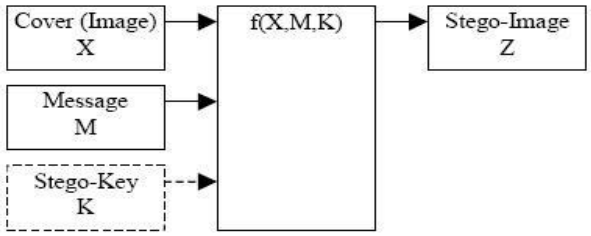


Figure1: Basic digital Steganography Encoder

## III. STEGANOGRAPHY IN IMAGE SPATIAL DOMAIN

Steganography procedures that alter the cover picture and the mystery picture in the spatial space are known as spatial area techniques. It includes encoding at the LSBs level.

Least Significant Bit Substitution (LSB) [3] is the most ordinarily utilized stenographic strategy. The essential idea of Least Significant Bit Substitution incorporates the embedding of the mystery data at the bits which having least weighting with the goal that it won't influence the estimation of unique pixel.

Another steganographic strategy to conceal a mystery message into a dim - esteemed cover picture was proposed [4]. For embedding a mystery message, a cover picture is parceled into non-covering pieces of two successive pixels. In each square, a distinction esteem is ascertained from the estimations of the two pixels. At that point that distinction esteem is supplanted by another incentive to implant the estimation of the mystery message. This technique delivers a more indistinct outcome than those acquired from straightforward least-significant-bit substitution strategies. The inserted mystery message can be separated from the subsequent stego-picture without referencing the first cover picture.

Iuon-Chang Lin [5] proposed a Data concealing plan with twisting resilience which utilizes spatial area for concealing data. This strategy gives mutilation resilience and gives better nature of handled picture. This plan gives viable outcomes than different plans as far as contortion resilience.

As LSB inclusion is more straightforward and useful for steganography, we can attempt to enhance one of its real downsides: the simplicity of extraction. We don't need that a meddler has the capacity to peruse all that we are sending.

## IV. STEGANOGRAPHY IN FREQUENCY DOMAIN

The necessity for updated security, has provoked the change of various figurings. LSB strategy has weak insurance from strikes. So to vanquish this inadequacy, researchers found a predominant course to conceal information in zones of the photo that are less introduced to weight, altering, and picture taking care of.

A lossless and reversible steganography plan has been exhibited that use each bit of quantized discrete cosine change (DCT) coefficients in JPEG pictures for implanting riddle information [6]. In this arrangement, the two dynamic zero coefficients of the medium-repeat parts in each piece are used to cover the puzzle information. This system achieves a high picture nature of stego picture and successfully achieves reversibility.

A reversible information disguising plan that uses the histogram moving strategy in light of DCT coefficients was proposed [7]. Cover pictures are allocated a couple of novel frequencies, and the high-repeat parts are used for installing the puzzle information. For disguising riddle information, this system for histogram moving developments the positive coefficients around zero to the other side and the negative coefficients around zero to the lef . It upgrades as far as possible and nature of the stego-pictures. On exchanging the repeat region stego-picture back to the spatial space picture may cause undercurrent and surge issues.

Wavelets change (WT) changes over spatial zone information to the repeat space information. Wavelets are used as a piece of the photo steganographic appear in light of the way that the wavelet change unmistakably divides high-repeat and low-repeat information on a pixel by pixel introduce. Various utilitarian tests propose to use the Wavelet change zone for steganography because of different purposes of intrigue. The usage of such change will generally address the point of confinement and generosity of the Information Hiding structure features.

A Haar discrete wavelet change (HDWT)- based reversible information covering procedure was proposed in 2009 [8]. In this system a spatial space picture is changed into a HDWT-based repeat zone picture and after that the high repeat coefficients are used to embed the puzzle information. This procedure gives a high disguising limit and a not too bad stego-picture quality.

In the present year DWT based estimation for picture information stowing endlessly has been prescribed that uses CH band of cover picture for disguising the riddle message. Vijay kumar [9] proposed a count in which puzzle message is introduce in different gatherings of cover picture. PSNR has been used to measure the idea of stegano picture and it gives better PSNR by supplanting botch ruin with cockeyed detail coefficients (CD) as stand out from various coefficients.

Another photo steganography technique in light of Integer Wavelet Transform (IWT) and Munkres' undertaking computation was introduced [10]. IWT changes over spatial space information to the repeat territory information. For implanting puzzle information, assignment computation is used for best planning between squares. Stego picture is subjected to various types of picture planning attacks and it shows high power against these ambushes.

Prabakaran G. [11] proposed a steganography approach for disguising a gigantic size puzzle picture into a little size cover picture. Arnold change is performed to scrambles the secret picture. Both riddle and cover pictures are rotted using

discrete wavelet change (DWT) and took after by Alpha blending movement. Discrete wavelet coefficients are used for covering the information to grow as far as possible. This DWT based approach gives high security and certain power.

As an execution measure for picture bending in light of inserting, the remarkable apex movement to racket extent (PSNR), which is masterminded under difference mutilation estimations, can be associated with stego pictures.

$$PSNR = 10\log(\frac{C_{max}^2}{MSE})$$

Where MSE denotes the mean square error, which is given as

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2$$

## V. ADAPTIVE STEGANOGRAPHY

Flexible steganography is an extraordinary occurrence of the spatial and change methods. Moreover, it is introduced as estimations careful inserting and hiding. Overall authentic characteristics of the photo are basically used before any undertaking to deal with its repeat changed coefficients. These bits of knowledge pick what changes can be made. An unpredictable flexible selection of pixels truly depicts this methodology, contingent upon the cover picture and the assurance of pixels in a square with a far reaching standard deviation (STD). The latter is wanted to avoid regions of uniform shading, for instance, smooth zones. This system is known for manhandling pictures with existing or intentionally included commotion and with pictures that show shading unconventionality [12-15]

A flexible slightest huge piece (LSB) steganographic technique was proposed [16]. This methodology fuses pixel-regard differencing (PVD) which uses the qualification estimation of two progressive pixels to evaluate what number of secret bits will be introduced into the two pixels. The PVD approach is used to isolate the smooth and edge zones. A k-bit LSB substitution system is used for disguising information in the pixels arranged in the edge zones. The extent of refinement regards is adaptively isolated into three one of a kind levels that are cut down level, focus level, and more raised sum. This system achieves greater payload utmost and high picture quality.

Another procedure which makes usage of also incorporating pixels around a target pixel to find the most fitting cutoff a motivator remembering the ultimate objective to improve vagary was displayed [17]. As diverge from other steganographic strategies which use either three or four bordering pixels around a goal pixel, this framework can utilize each one of the eight adjoining neighbors, which upgrades the vagary regard.

## VI. ANALYSIS

Three common requirements, security, capacity, and imperceptibility, may be used to rate the performance of steganographic techniques.

Where $x$ and $y$ are the image coordinates, $M$ and $N$ are the dimensions of the image, $S_{xy}$ is the generated stego-image and $C_{xy}$ is the cover image. Also $C_{max}^2$ represents the maximum value in the image.

The other Image quality parameters are normalized cross correlation, average difference, and maximum difference [11].

- Normalized cross correlation (NCC) is defined as in (1)

$$NCC = \sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})\frac{1}{\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k}^2)} \quad (1)$$

- Average difference (AD) is defined as in (2)

$$AD = \sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})/_{MN} \quad (2)$$

- Maximum difference (MD) is defined as in (3)

$$MD = Max(|x_{j,k} - x'_{j,k}|) \quad (3)$$

The original cover image $x$ sized $M \times N$ and the stego image $x'$ sized $M \times N$, and the $x_{j,k}$ and $x'_{j,k}$ are pixel located at the $i^{th}$ row and the $k^{th}$ column of images $x$ and $x'$, respectively.

Spatial domain techniques have large payload but often offset the statistical properties of the image. It is not robust against lossy compression, image filters, rotation, cropping and translation noise. 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.

DCT based domain techniques are less prone to attacks than the spatial domain methods at the expense of capacity. It is not robust against rotation, cropping and translation. Embedding in the DWT domain gives better result [18].

## VII. LITERATURE SURVEY

The main purpose of this paper is to present a survey on various steganography techniques used in recent years.

Table 1 presents an extensive literature survey in which all the papers are arranged in a descending order of their year of publication. Different techniques were used by different authors in different years were mentioned clearly along with their advantages and limitations.

TABLE 1: Comparison Table

| Author | Steganography techniques and other technical details | Limitations | Advantages |
|---|---|---|---|
| Alam and Islam 2013 [19] | SDS, ATMED, ATMAV, MED. Color Quantization: 256 colors, 240 blocks, RGB components- 3 bit R, 2 bit G and 3 bit B component. | PSNR ratio performance is not very much good and not effective for standard datasets. | To compare the accuracy of the transmitted data, safe and secure image data transformation and to authenticate the sender SDS is efficiently incorporated. |
| P. Kadam, A. Kandhare, M. Nawale, and M. Patil 2013 [20] | AES:- 128 bit key,32-bit words,128-bit cipher key, LSB, Experimental design: Intel core i3 at 2.27GHz, 4GB RAM, 500GB hard disc capacity. | Memory required for implementation should be as small as possible. | Prevent transformation of secrete file from third party access, Increased data security level and Keys of decryption process is protected from the hackers. |
| S. Mahato,D. K Yadav, and D. A Khan 2013 [21] | HTML attributes, Stegno-Crypto techniques. | Secrete message can't be extracted and High time complexity of the algorithm. | Steganography is achieved easily by HTML as HTML is rich in code and very less chance to check its source code and easily communicated through internet. |
| M. K Ramaiya, N. Hemrajani, and A. K Saxena 2013 [22] | LSB:- 2-bit, DES:- 64-bit,16 rounds, S-Box: - 6-bit as input and 4- bit output, 4*16 definition tables,0-15 decimal values. | Small modification to an S-Box could significantly weaken DES. | In presented paper, high level of security is provided and variation in two LSB of each pixel will not affect the cover image quality. |
| Y. J Chanu, T. Tuithung, and K. M Singh 2012 [23] | RS method, Spatial domain, Transform domain. . | Not able to detect the secret message | All strong and weak points are mentioned very clearly and by analyzing steganalysis techniques a better steganography techniques can be developed. |
| S. F. Mare, M. Vladutiu, and L. Prodan 2012 [24] | LSB:- 9 LSBs RGB images, Payload adaptation. | Jump table cannot be store in nosy areas. | Stronger steganographic model. Size of jump table for extraction is reduces and leaves more space for secret data |
| Utsav Seth and Shiva Saxena 2016 [25] | Advanced Encryption System | 50.15 db PSNR, 0.627 MSE, 128 bytes data | High data capacity and high security |
| Shruti C.Dande, Sushma Agrawal, Sunil Hirekhan 2016 [26] | LSB Insertion method | 64.537 db PSNR | High Security |
| Irshad Ahmed Ansari, 2016 [27] | DWT based on SVD and ABC | cost of computation may be higher | Auto calculation and user defined imperceptibility level |
| Sajjad Dadkhah, 2014 [28] | SVD based block feature computation | noise/blur near edges of images or video frames | it is better for collage attack and constant-average attack |
| Min jae, 2016 [29] | SVD Based Adaptive QIM Watermarking | _____ __ | robust against volumetric attack |
| A.R. Elshazly, 2016 [30] | combination of DWT+SVD+QIM | highly computation intensive | _____ __ |

## VIII. CONCLUSION

The fundamental reason for this paper is to display a study on different steganography procedures utilized as a part of late years. Table 1 shows a broad writing study in which every one of the papers are masterminded in a diving request of their time of distribution. Diverse strategies were utilized by various creators in various years were specified unmistakably alongside their points of interest and impediments.

The promising methodologies, for instance, DCT, DWT and the flexible steganography are not slanted to ambushes, especially when the hid message is nearly nothing. They change the coefficients in the change zone, therefore realizes minimum picture distortion. Generally, such strategies tend to have a lower payload when they are appeared differently in relation to the spatial territory figurings. The tests on the discrete cosine change (DCT) coefficients have introduced some reassuring results and after that they have involved the examiners' thought towards JPEG pictures. Working at some level like that of DCT turns steganography significantly more successful and less slanted to quantifiable ambushes. Inserting in the DWT space reveals a sort of valuable results and beats DCT installing.

## IX. REFERENCES

[1] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[2] S.B. Sadkhan., "Cryptography: Current status and future trends", in Proc. IEEE Conference on Information &

Communication Technologies, 2004, pp. 417-418.
[3] Chan, C.K., Chang, L.M., "Hiding data in image by simple LSB substitution", Pattern Recognition, vol 37, pp.469-471, 2003.
[4] Da-Chun Wu, Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters 24 (2003) 1613–1626.
[5] I.-C. Lin et al, "Hiding data in spatial domain images with distortion tolerance", Computer Standards & Interfaces 31 (2009) 458–464.
[6] C.-C. Chang et al., "Reversible hiding in DCT-based compressed images", Information Sciences 177 (2007) 2768–2786.
[7] Yih-Kai Lin, "High capacity reversible data hiding scheme based upon discrete cosine Transformation", The Journal of Systems and Software 85 (2012) 2395– 2404.
[8] Y.-K. Chan et al, "A HDWT-based reversible data hiding method", The Journal of Systems and Software 82 (2009) 411–421
[9] Vijay Kumar and Dinesh Kumar, "Performance Evaluation of DWT Based Image Steganography", 2010 IEEE 2nd International Advance Computing Conference
[10] N Raftari, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", 2012 Sixth Asian Modelling Symposium.
[11] 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].
[12] E. Franz and A. Schneidewind., "Adaptive steganography based on dithering", in Proc. Of the 2004 workshop on Multimedia and Security, 2004. pp. 56-62.
[13] R. Bohm and A. Westfeld, "Breaking cauchy model-based JPEG steganography with first order statistics", In Proc. of ESORICS'2004, 2004. pp. 125-140.
[14] 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.
[15] 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 spatial LSB domain systems", IEEE transactions on information forensics and security, vol. 3, no. 3, september 2008.
[17] Masoud Afrakhteh and Subariah Ibrahim, "Adaptive Steganography Scheme Using More Surrounding Pixels", IEEE International Conference On Computer Design And Appliations (2010).
[18] Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010), "Digital image steganography: survey and analysis of current methods", Signal Processing Journal. [On line]. 90(3), pp.727-752. Available: http://www.abbascheddad.net/Survey.pdf [Aug. 2011].
[19] F. I Alam, and M. M Islam,"An investigation into image hiding steganography with digital signature framework," Informatics, Electronics & Vision (ICIEV), 2013 international conference on 17-18 May 2013, page(s):1-6.
[20] P. Kadam, A. Kandhare, M. Nawale, and M. Patil, "Separable reversible encrypted data hiding in encrypted image using AES algorithm and lossy technique, "Pattern recognition, Informatics and medical engineering (PRIME), 2013 international conference on 21-22 Feb. 2013,page(s):312-316.
[21] S. Mahato,D. K Yadav, and D. A Khan," A modified approach to text steganography using hypertext markup language," Advanced computing and communication technologies (ACCT), 2013 third international conference on 6-7 April 2013, page(s):40-44.
[22] M. K Ramaiya, N. Hemrajani, and A. K Saxena," Improvisation of security aspect in steganography applying DES," Communication systems and network technologies (CSNT), 2013 international conference on 6-8 April 2013, page(s):431-436.
[23] Y. J Chanu, T. Tuithung, and K. M Singh," A short survey on image steganography and steganalysis techniques," Emerging trends and applications in computer science (NCETACS), 2012 3rd national conference on 30-31 March 2012,page(s):52-55.
[24] S. F. Mare, M. Vladutiu, and L. Prodan,"High capacity steganographic algorithm based on payload adaptation and optimization,"Applied computational intelligence and informatics (SACI), 2012 7th IEEE international symposium on 24-26 May 2012,page(s):87-92.
[25] Utsav Seth et. al, "Image Steganography Using AES Encryption and Least Significant Nibble", IEEE, Pp 2876-0879, 2016.
[26] Shruti C.Dande, "Implementation of color image steganography using LSB and Edge Detection Technique: A Lab View Approach", IEEE, Pp 1466-1469, 2016.
[27] Irshad Ahmad Ansari , Millie Pant et al Multipurpose Image watermarking in the domain of DWT based on SVD and ABC, *Pattern Recognition Letters* (2016)
[28] Sajjad Dadkhah et al "An effective SVD-based image tampering detection and self-recovery using active watermarking" (2014)
[29] Min Jae et al "SVD Based Adaptive QIM Watermarking on Stereo Audio Signals" (2016)
[30] A R Elashlzy "Synchronized Double Watermark Audio Watermarking Scheme Based on a Transform Domain for Stereo Signals", (2016).