http://www.jctjournals.com ISSN(ONLINE):2278 – 3814

Volume-10, Issue-2,February, 2020
JOURNAL OF COMPUTING TECHNOLOGIES (JCT)
International Journal
Page Number: 01-05

A Literature Survey on Stenography Approach Based on Different LSB Technique

K Saraswati [1], Prof. Sumit Sharma[2]
M.Tech Student CSE[1], Head of Computer Science Engineering[2]
[1,2]Vaishnavi Institute of Technology & Science Bhopal (M.P), India
swatisheetal1820@gmail.com

***Abstract*—In today world digital Image processing is used in many fields like computer vision, remote sensing, medical imaging, robotics, satellite images and aerial photography etc. There are different Data hiding scheme and techniques are available for shield creation. Steganography is the fine art for encryption of the confidential data in cover media to protect such data that are hack by hacker. The main purpose of steganography is, hiding the existence of the actual communication. In steganography, data can be hidden in carriers such as image, audio files, text files and video files. In this survey paper discuss the different methods based on LSB technique. There are different LSB different are available Random Invert LSB and another LSB techniques. In this paper discuss the different LSB techniques. MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two common quality measurements to measure the difference between the cover-image and the stego-image. Image-based data hiding techniques are secure but day to day size of secret data is increasing day by day.**

Keywords - Data Hiding, Steganography Random Invert LSB and LSB.

I. INTRODUCTION

An With advancements in digital communication technology and thus the extension of PC power and storage, the complications in ensuring persons' privacy become more and harder. The degrees to that people appreciate privacy dissent from one person to another. Numerous strategies are investigated and developed to shield personal privacy. Encoding is perhaps the most obvious one, and then comes steganography. This position is kind of different from the perspective taken with cryptography as an example. Governments invested with vast money and resources to create an unbreakable encoding algorithmic program. This has never been the case with steganography. Questions arise, like whether child pornography exists inside apparently innocent image or audio files? Are criminal's transmissions their secret messages in such a way? Are anti-virus systems fooled every time by secret embedding? The answers are still not trivial. However, what's evident is that steganography will have some useful applications, and like alternative technologies, like encryption, it may be exploited. This thesis advocates the importance of steganography not just for secure personal communication however together for a variety of other applications like digital forgery detection and lost signals reconstruction.

In recent years digital image-based steganography has established itself as a vital discipline in signal processing. That's due partly to the robust interest from the analysis community. Unfortunately, given the high volume of the presented methods, the literature wants a comprehensive review of these evolving strategies. All of the prevailing strategies of steganography concentrate on the embedding strategy and provides no consideration to the per-processing stages, like cryptography, as they depend heavily on the traditional cryptography algorithms which obviously aren't tailored to steganography applications where flexibility, strength and security are needed, a steganography scholar at Dresden University, , known as upon researchers in the field to analyze the interaction between steganography and cryptography, the crypto-Stego interface. Many of the existing approached assumes that flexibility to noise, double compression, and different image processing manipulations aren't required in the steganography context. As such, within the warden passive attack scenario their hide information will be destroyed or won't be recoverable. Adjustive steganography aimed toward distinguishing textural or quasi-textural areas for embedding the secret information runs into a few problems

at the decoder aspect since its classification algorithms aren't salient. During this thesis, skin-tone areas are the preferred selection for texture detection since the detection algorithmic rule is robust and distinctive. Furthermore, skin-tone regions continuously show chrominance standards exist in on a middle range, hence, the issue of underflow or overflow is overwhelmed automatically. Within the methodology of finding out a good skin-tone detection algorithmic rule, the various accessible techniques are established to either be slow in execution and/or accompany intolerable false alarms. Often, these algorithms neglect the fact that luminance can facilitate improve their performance.

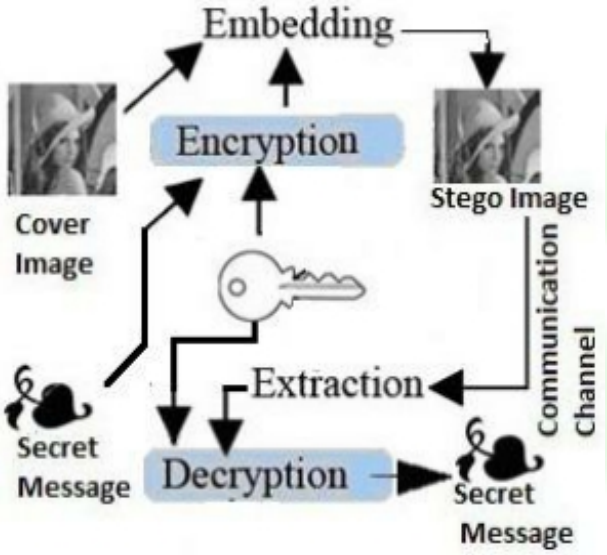

Fig.1 Block Diagram of Steganography

II. LITERATURE SURVEY

Prabhash Kumar Singh et.al [2020], "Superpixel based robust reversible data hiding scheme exploiting Arnold transform with DCT and CA", in this presented by author a eminent data hiding technique is developed using super pixels to ease the hiding of data at the corresponding blocks of the Cb and Cr colour components through DCT and CA. The labelled image of super pixel is taken into consideration to classify a block as heterogeneous or homogeneous. The proposed method of implementation was found to be more optimal than the four possible methods after making a trade-off between visual quality (PSNR) and embedding bits (capacity). The selected method achieved an average PSNR of 49 dB with a relatively high embedding bit on a standard database image. Moreover, the scheme performed significantly better than all state-of-the-art schemes on common images. Further, various experiments and analysis are conducted to show the efficacy of the proposed method.The stated method is tested to determine the robustness and visual quality of the stego image under different geometric and non-geometric attacks. The secret image is recovered within an acceptable condition even after the tampering of the stego images. Security of the proposed scheme is enhanced by employing Arnold transform which utilizes sharable keys to determine the sequence of order of selection of blocks for data hiding. A user will not be able to obtain the secret image with invalid keys even if it knows the algorithm. Thus, the proposed scheme will serve the need for secret data communication and ownership authorization in different institutions and organizations such as health care, courts of law, and in securing of intellectual property. Nevertheless, the proposed scheme needs to be enhanced in the future course of work for high embedding capacity, robustness against JPEG compression, and vector quantization along with self-recovery properties [01].

Arunkumar et.al,[2019],"SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images", in this presented by author A robust image steganographic scheme based on RIWT, DCT and SVD has been proposed in our paper. This scheme has combined the technology of RIWT, DCT, the SVD decomposition technique and the logistic chaotic map. As RIWT is a shift invariant, reversibility and robustness are achieved in our proposed scheme. Better imperceptibility is achieved by using SVD and DCT, as embedding is completed on singular values. Usage of the logistic chaotic map to encrypt secret medical images provides extra security and also improved robustness to our scheme. As decomposition is done using SVD and embedding is done on a specific sub band of decomposed block, steganalysis has become a tough task. Moreover, modification of the SVs of SVD efficiently resists geometric attacks and attacks by image manipulation. The experimental results, as well as the analysis and comparison with similar schemes in the literature, show that our scheme is superior to other schemes in terms of imperceptibility, reversibility and robustness. Confidentiality is a key requirement in healthcare areas such as Telemedicine. The medical image needs to be secured during transmission. Authentic images and their integrity are prime requirements in healthcare. This proposed method can provide authenticity and integrity of the medical images in the transmission process, and cryptography can ensure the confidentiality of these medical images. The method can be used for Military applications too, where secrecy is a must. In the future, we plan to enhance the steganography framework by embedding secret medical image blocks only in few cover image blocks based on statistical measure like contrast and correlation[02].

Aniruddha Kanhe et.al [2018], "Robust image-in-audio watermarking technique based on DCT-SVD transform" in this presented by author a novel audio watermarking technique based on DCT and SVD transform. The proposed technique embeds the watermark bits adaptively in selected frames having low frequency and high energy. The

watermark bits are embedded in DCT coefficients of selected frames by performing SVD operation. The watermark bits are embedded in non-diagonal elements of SVD matrix. Experiments are conducted to evaluate the performance of the proposed audio watermarking technique and compared with recent frequency-domain audio watermarking techniques. The high-SNR values confirm that the proposed technique is highly imperceptible. The robustness of proposed audio watermarking technique is evaluated by computing BER and AIL for re-sampling, re-quantization, AWGN, and MP3 compression attacks with high data payload. The proposed watermarking scheme achieves comparable, if not better, results compared with other recently developed techniques for various attacks considered in this work. Future research work may include the enhancement of proposed technique to withstand with random cropping attack, pitch shifting attack, and time-scale modification attack. The proposed technique can be made robust against these attacks by embedding synchronization codes with watermark bits[03].

Rupali Bharadwaj et.al [2016],"Image steganography based on complemented message and inverted bit LSB substitution." in this presented by author an three stage complementing the secret message in First stage, then using pseudo random number generator data are selected randomly and hiding complemented secret message in cover image pixels in second stage and in third stage inverted bit LSB use as steganography rather than simple LSB used, thus, it provide maximum security and less chance to eavesdrop or detect the error. Experimental study proofs the proposed system is better than basic LSB in term of higher PSNR value of hiding secrete message in the cover image thus it overcome the chance of attack on the communication and attacker cannot easily detect the original message[04].

Nadeem Akhtar,et.al [2014] "An improved inverted LSB image steganography. In Issues and Challenges in Intelligent Computing Techniques "in this presented by an An Improved Inverted LSB Image Steganography: In this paper, a change in the plain LSB based picture steganography is proposed and actualized. The paper proposes the utilization of bit reversal method to enhance the stegoimage quality. Two plans of the bit reversal procedures are proposed and executed. In these strategies, LSBs of a few pixels of cover picture are reversed on the off chance that they happen with a specific example of a few bits of the pixels. Along these lines, less number of pixels is altered in contrast with plain LSB strategy. So PSNR of stegoimage is moved forward. For right de-steganography, the bit designs for which LSBs has upset should be put away inside the stego-image some place. The proposed bit reversal strategy gives great change to LSB steganography. This technique could be combined with other methods to improve the steganography further [06].

Cheng-Hsing ,et.al,[2008], "Adaptive data hiding in edge areas of images with spatial LSB domain systems", in this presented by author In an a new adaptive least-significant bit (LSB) stenographic method using pixel-value difference (PVD) that provides a larger embedding capacity and imperceptible stego-images. The method exploits the difference value of two consecutive pixels to estimate how many secret bits will be embedded into the two pixels. Pixels located in the edge areas are embedded by a -bit LSB substitution method with a larger value of than that of the pixels located in smooth areas. The range of difference values is adaptively divided into lower level, middle level, and higher level. For any pair of consecutive pixels, both pixels are embedded by the -bit LSB substitution method. However, the value is adaptive and is decided by the level which the difference value belongs to. In order to remain at the same level where the difference value of two consecutive pixels belongs, before and after embedding, a delicate readjusting phase is used[07].

Xinpeng Zhang[2004],et.al , "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security" in this presented by author The pixel valued differencing (PVD) steganography can implant a lot of mystery bits into a still picture with high subtlety as it makes utilization of the attributes of human vision affectability. Be that as it may, an escape clause exists in the PVD strategy. Unordinary ventures in the histogram of pixel contrasts uncover the nearness of a mystery message. An examiner can even gauge the length of concealed bits from the histogram .To improve security, a changed plan is proposed which keeps away from event of the previously mentioned ventures in the pixel contrast histogram while safeguarding the upside of low visual contortion of the PVD. The histogram-based steganalysis is in this way vanquished. Since a bigger number of information are installed into occupied regions than into smooth ranges, the pixel-esteem differencing steganography has a decent impalpability and extensive implanting limit. However, the abnormal behaviour of the pixel difference histogram reveals the presence of hidden message. After detecting the steps in the histogram, a steganalyst can further estimate the amount of embedded bits. The original PVD method is still vulnerable to the histogram analysis described in this paper even if a pseudo-random pattern is used in defining the pixel doublets. To enhance security, it is proposed to introduce a pseudo-random dithering to the division of ranges of the pixel-value differences. This successfully evacuates the undesirable strides existing in the PVD histogram of the stego-picture acquired utilizing the first strategy. Along these lines, the histogram based steganalysis is crushed while the benefits of substantial implanting limit and high imperceptibility of the first PVD are protected**[08].**

Andrew D. Keret.al , [2004], "Improved detection of LSB steganography in grayscale images." in this presented by author We consider strategies for noting dependably the subject of whether a picture contains concealed information; the emphasis is on dark scale bitmap pictures and basic LSB steganography. Utilizing an appropriated calculation organize and a library of more than 30,000 pictures we have been painstakingly assessing the dependability of different steganalysis strategies. The outcomes recommend various enhancements to the standard systems', with specific advantages picked up by not endeavoring to assess the shrouded message length. Broad experimentation demonstrates that the enhanced techniques permit solid identification of LSB steganography with in the vicinity of 2 and 6 times littler inserted messages. We conclude with a summary of the improvements made by these new detection statistics. It is necessary to simplify, so we have used a definition of "reliable" detection as meaning 5% false positives and at most 50% missed detections (we recognize that these figures are arbitrary but they are in reasonably useful for an Information Security Officer who would only make a definite diagnosis of steganography after seeing a number of positive results coming from the same person). We measured the lowest level of steganography for which such reliability is attained by each statistic, repeating for each Image Set, and also subjected the covers of Image Set A to JPEG compression at mild (quality factor 90), moderate (75) and strong (50) levels so Above, the results of segmentation. Below, ROC curves showing the benefits; the statistic used is the non-overlapping version of the relative difference between R and R_, as computed using the mask [0, 1, 1, 0]. The segmenting statistic takes the 30th percentile of the estimates for each segment. 3% steganography was embedded as to examine this factor. The segmenting statistic was not tested against Image Set A because initial results showed no likelihood of improvement**[09].**

Da-Chun Wuet.al , [2003] "A steganographic method for images by pixel-value differencing." in this presented by authorIn Another and conservative stegano-realistic strategy for implanting mystery messages into a dim esteemed cover picture is anticipated. Inside the strategy for installing a mystery message, an overhang picture is partitioned into non-covering pieces of two sequential pixels. A distinction cost is ascertained from the estimations of the two pixels in each square. All conceivable refinement qualities are arranged into various extents. The choice of the vary intervals is based on the characteristics of human vision's sensitivity to grey price variations from smoothness to distinction. The distinction price then is replaced by a replacement price to imbed the worth of a sub-stream of the key message. The quantity of bits which might be embedded in a constituent try is set by the breadth of vary that the distinction price belongs to. The tactic is meant in such the way that the modification isn't out of the vary interval. This technique provides essay straightforward, thanks to turn out additional invisible result than those yielded by simple least-significant-bit replacement methods. The installed mystery message can be separated from the subsequent stego-picture without referencing the first cover picture. In addition, a pseudorandom system might be utilized to accomplish mystery security. Trial comes about demonstrate the possibility of the proposed Method. Double measurements assaults were likewise directed to gather related information to demonstrate the security of the strategy. Another and effective PC based stenographic strategy for inserting mystery messages into pictures without delivering detectable changes has been proposed. There is no need of referencing the first picture while separating the inserted information from a stego-picture. The technique uses the normal for the human vision's affectability to dark esteem varieties. Mystery information are implanted into a cover picture by supplanting the distinction estimations of the two-pixel squares of the cover picture with comparative ones in which bits of inserted information are incorporated. The strategy not just gives a superior approach to installing a lot of information into cover pictures with imperceptions, additionally offers a simple approach to finish mystery. This embedding method can be easily extended to efficiently carry content-related messages such as captions or annotations in audios and videos by embedding data in each adjacent pair of signals of the data-streams **[10].**

IV. Conclusion and Future Work

Digital Steganography is an engrossing scientific area which comes under the security system. In this paper, Steganography use based pixel identification and embed the secret data using proposed methodology. PSNR values and Data hiding capacity both parameters are inversely proposal. Peak signal to noise ratio based comparison is important for pixel value based method. In this paper compare different methods pixels based method.

REFERENCES

[1] Singh, Prabhash Kumar, Biswapati Jana, and Kakali Datta. "Superpixel based robust reversible data hiding scheme exploiting Arnold transform with DCT and CA." *Journal of King Saud University-Computer and Information Sciences* **(2020).**

[2] Arunkumar, S., V. Subramaniyaswamy, V. Vijayakumar, Naveen Chilamkurti, and R. Logesh. "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images." *Measurement* 139 **(2019):** 426-437.

[3] Kanhe, Aniruddha, and Aghila Gnanasekaran. "Robust image-in-audio watermarking technique based on DCT-SVD transform." *EURASIP Journal on Audio, Speech, and Music Processing* 2018, no. 1 **(2018):** 1-12.

[4] Shete, Kalpana Sanjay, Mangal Patil, and J. S. Chitode. "Least significant bit and discrete wavelet transform algorithm realization for image

steganography employing FPGA." *International Journal of Image, Graphics and Signal Processing* 8, no. 6 **(2016):** 48.

[5] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal o Computer Science and Engineering, IJCSE, vol. 1, no. 3, **(2009)**.

[6] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. **(2008)** September 3, pp. 488-497.

[7] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), **(2008)** August 28-30, pp. 355-358.

[8] H. Zhang, G. Geng and C. Xiong, "Image Steganography Using Pixel-Value Differencing", Electronic Commerce and Security, ISECS '09. Second International Symposium on **(2009)** May.

[9] Wu D, Tsai W. A stenographic method for images by pixel value differencing. Pattern Recognit. Lett. **(2003)**; 24:1613–1626.

[10] Zhang X, Wang S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Lett. **(2004);** 25: 331–339.

[11] Ker A. Improved detection of LSB steganography in grayscale images. In Proc. Information Hiding Workshop Springer LNCS**(2014)**; 3200: 97–115.

[12] Yang HC, Weng CY, Wang SJ, Sun HM. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. Inf. Forensics Security **(2008)**; 3: 488–497.

[13] Akhtar N, Khan S, Johri P. An improved inverted LSB image steganography. In Issues and Challenges in Intelligent Computing Techniques (ICICT), International Conference on. IEEE,**(2014)**; p. 749-755.

[14] Rupali Bhardwaj, Vaishali Sharma, "Image Steganography Based on Complemented Message and Inverted bit LSB Substitution" Elsevier, **(2016).**

[15] Chetan, K., Nirmala, S., 2015. An efficient and secure robust watermarking scheme for document images using integer wavelets and block coding of binary watermarks. J. Inf. Secur. Appl. **(2015)** 24, 13–24.

[16] Chowdhuri, P., Jana, B., Giri, D., 2018. Secured steganographic scheme for highly compressed color image using weighted matrix through dct. Int. J. Comput. Appl., 1–12,**(2018)**

[17] Chowdhuri, P., Pal, P., Jana, B., 2019. Improved data hiding capacity through repeated embedding using modified weighted matrix for color image. Int. J. Comput. Appl. 41, 218–232.**(2019)**

[18] Codella, N.C., Gutman, D., Celebi, M.E., Helba, B., Marchetti, M.A., Dusza, S.W., Kalloo, A., Liopyris, K., Mishra, N., Kittler, H., et al., 2018. Skin lesion analysis toward melanoma detection: a challenge at the 2017 international symposium on biomedical imaging (isbi), hosted by the international skin imaging collaboration (isic). In: 2018 IEEE 15th International Symposium on Biomedical Imaging **(ISBI 2018),** IEEE. pp. 168–172..

[19] Das, C., Panigrahi, S., Sharma, V.K., Mahapatra, K., 2014. A novel blind robust image watermarking in dct domain using inter-block coefficient correlation. AEU Int. J.Electron. Commun. 68, 244–253.**(2014.)**

[20] Dey, N., Das, P., Roy, A.B., Das, A., Chaudhuri, S.S., 2012. Dwt-dct-svd based intravascular ultrasound video watermarking. In: 2012 World Congress on Information and Communication Technologies, IEEE. pp. 224–229**.(2012)**.

[21] Dey, N., Maji, P., Das, P., Biswas, S., Das, A., Chaudhuri, S.S., 2013a. An edge based blind watermarking technique of medical images without devalorizing diagnostic parameters. In: 2013 International Conference on Advances in Technology and Engineering (ICATE), IEEE. pp. 1–5.. **(2013)**

[22] Dey, N., Samanta, S., Yang, X.S., Das, A., Chaudhuri, S.S., 2013. Optimisation of scaling factors in electrocardiogram signal watermarking using cuckoo search. Int. J. Bio-Inspired Comput. 5, 315–326.**(2013)**

[23] Ekodeck, S.G.R., Ndoundam, R., 2016. Pdf steganography based on chinese remainder theorem. J. Inf. Secur. Appl. 29, 1–15. Fridrich, J., Goljan, M., Du, R., 2001. Invertible authentication. In: Security andWatermarking of Multimedia contents III, International Society for Optics and Photonics. pp. 197–208**(2016)**.

[24] Gupta, A.K., Raval, M.S., 2012. A robust and secure watermarking scheme based on singular values replacement. Sadhana 37, 425–440.Hamza, R., Hassan, A., Huang, T., Ke, L., Yan, H., 2019. An efficient cryptosystem forvideo surveillance in the internet of things environment. Complexity**(2019)**..

[25] Hamza, R., Yan, Z., Muhammad, K., Bellavista, P., Titouna, F., 2020. A privacypreservingcryptosystem for iot e-healthcare. Inf. Sci. 527, 493–510.**(2020.)**

[26] Jana, B., 2016. Dual image based reversible data iding scheme using weighted matrix. Int. J. Electron. Inf. Eng. 5, 6–19. Jana, B., Giri, D., Mondal, S.K., 2016. Dual-image based reversible datahiding scheme using pixel value difference expansion. IJ Network Secur. 18, 633–643**(2016)**.

[27] Jung, S.W., 2016. Lossless embedding of depth hints in jpeg compressed color images. Signal Process. 122, 39–51.**(2016.)**

[28] Kalra, G.S., Talwar, R., Sadawarti, H., 2015. Adaptive digital image watermarking for color

images in frequency domain. Multimedia Tools Appl. 74, 6849–6869.**(2015.)**

[29] Keshavarzian, R., Aghagolzadeh, A., 2016. Roi based robust and secure image watermarking using dwt and arnold map. AEU-Int. J. Electron. Commun. 70, 278–288**.(2016.)**

[30] Khare, P., Srivastava, V.K., 2020. An efficient image watermarking technique based on iwt-dct-svd. In: Advances in VLSI, Communication, and Signal Processing. Springer, pp. 841–849**.(2020)**

[31] Khashandarag, A.S., Navin, A.H., Mirnia, M.K., Mohammadi, H.H.A., 2011. Anoptimized color image steganography using lfsr and dft techniques. In: International Conference on Computer Education, Simulation and Modeling. Springer, pp. 247–253.**(2011)**

[32] Lin, C.C., Shiu, P.F., 2010. High capacity data hiding scheme for dct-based images. J.Inf. Hiding Multimedia Signal Process. 1, 220–240.**(2010)**

[33] Liu, C.L., Liu, H.H., 2013. Reliable detection of histogram shift-based steganography using payload invariant features. In: Applied Mechanics and Materials, TransTech Publ. pp. 3517–3521**(2013).**

[34] Molina-Garcia, J., Garcia-Salgado, B.P., Ponomaryov, V., Reyes-Reyes, R., Sadovnychiy, S., Cruz-Ramos, C., 2020. An effective fragile watermarking scheme for color image tampering detection and self-recovery. Signal Process. Image Commun. 81. 115725.**(2020.)**

[35] Muñoz-Ramírez, D.O., Ponomaryov, V., Reyes, R.R., Ramos, C.C., Sadovnychiy, S., 2019. Embedding a color watermark into dc coefficients of dct from digital images. IEEE Latin Am. Trans. 17, 1326–1334**.(2019.)**

