

Analytical Study of Spatial & Transform Domain Analysis of Image Stenography Techniques

Gurmeet Kaur, Rasneet Kaur, Amanpreet Kaur , Harpreet Kaur

Abstract

Data security is a standout amongst the most vital elements to be viewed when mystery data hosts as imparted between two gatherings. Cryptography and steganography are the two systems utilized for this reason. Cryptography scrambles the data, however it uncovers the presence of the data. Steganography conceals the genuine presence of the data so that any other person other than the sender and the beneficiary can't perceive the transmission. In steganography the mystery data to be imparted is covered up in some other transporter such that the mystery data is undetectable. This paper gives a relative investigation of various steganography strategies. At the point when the mystery data is covered up in the bearer the outcome is the stego flag. The nature of the stego picture is measured by Peak Signal to Noise Ratio (PSNR), MSE

Introduction

Over numerous years data security is the greatest test for analysts. Since cryptography can't make anything undetectable, it is swapped by steganography for concealed correspondence. Steganography conceals mystery data in different articles known as cover items. Cover questions alongside the concealed data is known as stego protest. The cover can be a picture, sound or video. The mystery can be instant message, picture or sound. In this paper the cover is a picture and mystery data is a sound document. The steganography is accomplished in change area. There are basically two sorts of steganography procedures: worldly area and change space. In worldly space, the real example qualities are controlled to conceal the mystery data. In change space, the cover protest is changed over to various area, for example, recurrence area, to get the changed coefficients. These coefficients are controlled to shroud the mystery data.

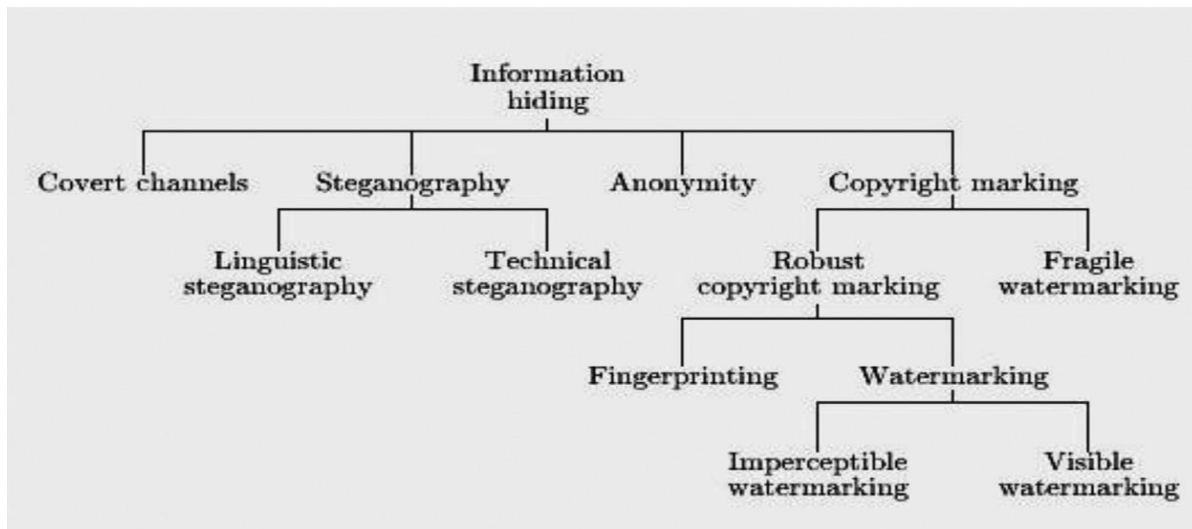


Fig -1: Information Hiding Techniques

2. Steganography techniques

In the course of the most recent decades, a few steganography calculations have been utilized to safeguard information security. These systems comprise of two spaces, which are: spatial area procedures and recurrence area methods.

2.1. Spatial domain techniques

Here spatial components of picture are utilized. This is a most straightforward steganographic system that implants the bits of mystery message specifically into the minimum critical piece (LSB) plane of the cover picture. In a dim level picture, each pixel comprises of 8 bits. The fundamental idea of LSB substitution is to install the private information at the furthest right (bits with the littlest weighting) so that the inserting strategy does not influence the first pixel esteem enormously [3]. The numerical portrayal for LSB is as condition 1:

$$x'_i = x_i - x_i \text{ mod } 2^k + m_i \dots\dots\dots(1)$$

In Equation (1), x'i represents the ith pixel value of the stego-image and xi represents that of the original cover image. mi represents the decimal value of the its block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as in equation 2:

$$m_i = x_i \text{ mod } 2^k \dots\dots\dots(2)$$

Hence, a simple permutation of the extracted mi gives us the original confidential data [5]. This method is easy and straightforward but this has low ability to bear some signal processing or noises and secret data can be easily stolen by extracting whole LSB plane. Although this method gives good results in terms of PSNR and MSE but it is more prone to attacks and can be easily detected that's why frequency domain methods are recommended to use for secure steganography

2.2 Steganography in Frequency Domain

Vigor of steganography can be enhanced if properties of the cover picture could be abused. Mulling over these viewpoints working in recurrence space turns out to be more alluring. Here, sender changes the cover picture into recurrence space coefficients before inserting mystery messages in it [4]. Utilizing change space procedures it is conceivable to insert a mystery message in various recurrence groups of the cover. These strategies are more unpredictable and slower than spatial area techniques; in any case they are more secure and tolerant to commotions. Recurrence area portrayals that have been widely utilized by the flag handling group [8].

2.2.1 The Discrete Cosine Transform (DCT) :This strategy is utilized, yet comparative changes are for instance the Discrete Fourier Transform (DFT). These numerical changes change over the pixels so as to give the impact of "spreading" the area of the pixel values over piece of the picture [5]. The DCT changes a flag from a picture portrayal into a recurrence portrayal, by gathering the pixels into 8 × 8 pixel squares and changing the pixel obstructs into 64 DCT.

The Two-Dimensional DCT

The 2-D DCT is a direct extension of the 1-D case and is given by

$$c(u) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos \left[\frac{\pi(2x+1)u}{2N} \right] \cos \left[\frac{\pi(2y+1)v}{2N} \right] \dots\dots\dots(3)$$

2.2.2 Discrete Wavelet Transform

Wavelets are extraordinary capacities which (in a frame closely resembling sins and cosines in Fourier examination) are utilized as basal capacities for speaking to signals. The discrete wavelet change (DWT) we connected here is Haar-DWT, the most straightforward DWT. In Haar-DWT the low recurrence wavelet coefficient are created by averaging the two pixel qualities and high recurrence coefficients are produced by taking portion of the distinction of a similar two pixels. A flag is gone through a progression of channels to compute DWT. System begins by passing this flag arrangement through a half band

advanced low pass channel with motivation reaction $h(n)$. Filtering of a flag is numerically equivalent to convolution of the tile motion with drive reaction of the channel.

$$x[n] * h[n] = \sum_{k=-\infty}^{\infty} x[k]h[n - k] \dots\dots\dots(4)$$

A half band low pass channel expels all frequencies that are above portion of the most elevated recurrence in the tile flag. At that point the flag is gone through high pass channel. The two channels are identified with each different as

$$h[L-1-n] = (-1)^n g(n)$$

Low Pass Rows Low Pass Cols	Low Pass Rows High Pass Cols
High Pass Rows Low Pass Cols	High Pass Rows High Pass Cols

Fig -2: DWT Sub Bands

For 2-D pictures, applying DWT (Discrete Wavelet Transform) isolates the picture into a lower determination estimate picture or band (LL) and flat (HL), vertical (LH) and corner to corner (HH) detail parts as appeared in figure.

4. REVIEW

This paper examinations the different papers on Spatial Domain and Transform Domain of Steganography strategies

Utsav Sheth and Shiva Saxena [4]paper portrays a steganography strategy in which content is hidden in a picture. The lower snack of each picture byte is changed to contain each snack of the information content. The steganography calculation utilized as a part of this execution amplifies on information limit and furthermore guarantees security.

H.B. Kekre, Archana Athawale, and Pallavi N.Halarnkar[10]proposes another enhanced rendition of Least Significant Bit(LSB) strategy. The approach proposed is basic for usage when contrasted with Pixel esteem Differencing (PVD) strategy and yetachieves a High installing limit and impalpability. The proposed technique can likewise be connected to 24 bit shading pictures and accomplish inserting limit considerably higher than PVD.

Mamta Juneja and Parvinder S. Sandhu[7]proposes an enhanced LSB(least Significant piece) based Steganography procedure for imagesimparting better data security .It introduces an inserting calculation for stowing away scrambled messages in nonadjacent and arbitrary pixel areas in edges and smooth territories of pictures. It initially scrambles the mystery message, and detectsedges in the cover-picture utilizing enhanced edge location filter.Message bits are then, installed at all critical byte of haphazardly chose edge territory pixels and 1-3-4 LSBs of red, green, blue parts individually crosswise over arbitrarily chose pixels crosswise over smooth range of picture.

Cheng Wei, Li Zhaodan [19]elaborates a calculation of vigorous picture watermarking mapping which is concentrate on implanting RGB watermark into RGB shading picture. The calculation depends on discrete wavelet change (DWT), discrete cosine change (DCT) and riotous framework. The pattern applies a self-adjusted watermark picture, as indicated by the shading picture R, G, B segments of the lightest weight determination. Watermark pictures scrambled by the strategic mappings. Due to the correlation between the low recurrence coefficients, DWT change will reinforce the estimations of

coefficient; consequently it is not profit of expanding the indistinctness of the watermarks. This paper utilizes the components of DCT to decrease the relationship between's DWT coefficients.

Barnali Gupta Banik [16]ensure unwavering quality and honesty in data transmission, picture steganography is bleeding edge innovation into day's advanced world. It can be actualized in spatial, time and recurrence area. In this examination article, a successful calculation has been presented which would insert mystery message information, mixed by Arnold Transform, in recurrence space utilizing the quantization coefficient change in Discrete Cosine Transform (DCT). At first the cover picture is part into pieces, then two dimensional DCT is connected on each picture square and changed mystery message is embedded by examining mid-band coefficients of DCT. After the fruitful transmission of the cover picture to the beneficiary, the mystery message can be viably recuperated in high caliber from the Stego picture.

3. MODEL

A. Definitions

(i) Cover image: It is defined as the original image into which the required information is embedded. It is also termed as carrier image. The information should be embedded in such a manner that there are no significant changes in the statistical properties of the cover image.

(ii) Stegoimage: It is a unified image obtained by the combination of the payload and cover image.

(iii) Perceptibility: It describes the ability of a third party (not the intended recipient) to visually detect the presence of hidden information in the stego image. The embedding algorithm is imperceptible when used on a particular image if an innocent third party, interested in the content of the cover image, is unaware of the existence of the payload. Essentially this requires that the embedding process not degrade the visual quality of the cover image.

(iv) Robustness: It characterizes the ability of the payload to survive the embedding and extraction process, even in the face of manipulations of the stego image such as filtering, cropping, rotating and compression.

(v) Security: It is inability of adversary to detect hidden images accessible only to the authorized user. The quality factor can enhance the security of the image. A steganographic image is perfectly secure when statistical data of the cover and stego images are identical

B. Error Analysis:

(i) Bit Error Rate: For the successful recovery of the hidden information the communication channel must be ideal but for the real communication channel, there will be error while retrieving hidden information and this is measured by BER. The cover image is represented as cov and stego image as steg in the given equation

$$BER = \frac{1}{|image^{covg}|} \sum_{i=0}^{all\ pixels} |image^{covg} - image^{steg}|$$

|Where i is the pixel position

(ii) Mean Square Error: It is defined as the square of error between cover image and the stego image. The distortion in the image can be measured using MSE.

$$\sum_{I=1}^{all\ pixels} \sum_{j=1}^{all\ pixels} \frac{(cov(i,j) - steg(i,j))^2}{N * N}$$

(iii) Peak Signal to Noise Ratio: It is the ratio of the maximum signal to noise in the stego image.

$$PSNR = 20 \log_{10} \frac{255}{\sqrt{MSE}}$$

Table 1: Comparison between schemes proposed by different researchers based on LSB, DCT and DWT

Sr no.	Author	Method	PSNR	MSE	Advantages
1	M. Juneja and P. S. Sandhu	LSB Method	69.12	0.52	High capacity, very good imperceptibility, Capacity
2.	Utsav Sheth and Shiva Saxena	LSB Method	50.15	0.62	High capacity, high security
3	Shahana T	DCT Method	61.433	0.42	High robustness, improved psnr
4	Barnali Gupta Banik, Samir Kumar Bandyopadhyay	DCT Method	47.86	0.92	Robustness,
5	Hamad A. Al-Korbi1, Ali Al-Ataby2, Majid	DWT(HAAR TRANSFORM)	55.78 (B&W)	0.171	Robustness, High Capacity
6	Umashankar Dewangan , Monisha Sharma , Swagota Bera	DWT Method	70.95	0.005	More security and payload capacity
7	Cheng Wei, Li Zhaodan	DWT-DCT	66.41	0.014	Robustness and payload capacity

CONCLUSIONS:

In this paper the different articles which are utilized spatial area and change space for picture covering up were contemplated and arranged. Steganography is a system of composing mystery message such a path, to the point that nobody can question for the presence of the message separated from the sender and considered beneficiary. In this paper, we think about picture Steganography procedures by utilizing LSB, DCT& DWT through MSE and PSNR. We have exhibited foundation exchange of DCT and DWT, calculation of Steganography and parameters for assessment of picture quality subsequent to inserting the information. From the outcomes, we get the conclusion that Spatial space steganography calculations are better in setting to the payload limit however they give less vigor where as Transform area watermarking calculations are better in setting to the power. The blend of the two changes enhanced the steganography execution significantly when contrasted with the DWT-Only steganography approach.

Acknowledgement





We are grateful to the Chandigarh engineering college, Landran , Mohali (Punjab) , affiliated to IKGPTU, (Kapurthala) for supporting our research work. The active and constant support of our research supervisors Dr. Ravinder Khanna & Dr. Manish Pandey being the main source of inspiration led this research a success.

REFERENCES:

- [1] Anil K Jain, "Fundamentals of Digital Image Processing", University of California-Davis, Prentice Hall, 1988
- [2] Ken Cabeen and Peter Gent, –Image Compression and Discrete Cosine Transform||, College of Redwoods. <http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/Fall98/PKen/dct.pdf>
- [3] H. V. Desai, "Steganography, Cryptography, Watermarking: A Comparative Study," Journal of Global Research in Computer Science, vol. 3, no. 12, pp. 33-35, 2012.
- [4]UtsavSheth and Shiva Saxena, "Image Steganography Using AESEncryption and Least Significant Nibble" International Conference on Communication and Signal Processing, April 6-8, 2016, India
- [4] M. A. Al-Tae, N. H. Al-Hassani, B. S. Bamajbour and D. Al-Jumeily, "Biometric-Based Security System for Plaintext E-mail Messages," in: Proc. International Conference on Developments in eSystems Engineering, Abu Dhabi, UAE, , pp. 1-6, 14 – 16 December 2009.

- [5] N. Qasrawi, M. A. Al-Tae, H. l'emair and R. Al-Asa'd, "Multilevel Encryption of Plaintext Messages Using a Smart Card Connected to PC Parallel Port," in: Proc. 3rd International Conference on Modelling, Simulation and Applied Optimization, Sharjah-UAE, , pp. 1-6, 20-22 January 2009.
- [6] S. Katzenbeisser and F. A. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Inc, 2000.
- [5] G. Swain and S.K. Lenka, "A Robust Image Steganography Technique Using Dynamic Embedding With Two Least Significant Bits," *Advanced Materials Research*, Vols. 403-408, pp.835-841, 2012.
- [7] M. Juneja and P. S. Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption," *Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing*, pp.302-305, 2009.
- [8] G. Swain and S. K. Lenka, "A Novel Steganography Technique By Mapping Words with LSB Array," *Signal and Imaging Systems Engineering*, Inderscience, e-ISSN: 1748-0701, p-ISSN: 1748-0698, 2012.
- [9] G. Swain and S. K. Lenka, "LSB Array Based Image Steganography Technique by Exploring the Four Least Significant Bits," *Proceedings of 4th International Conference, Obcom 2011, CCIS, 2012, Vol. 270, part II*, pp.479-488, 2011.
- [10] H. B. Kekre, A. A. Athawale and P. N. Halarankar, "Increased Capacity of Information Hiding in LSB's Method for Text in Image," *International Journal of Electrical, Computer and System Engineering*, Vol.2, No.4, pp.246-249, 2008
- [11] Dr. H. B. Kekre, Ms. Archana A. Athawale, "Information Hiding using LSB Technique with Increased Capacity", *International Journal of Cryptography and Security*, Special issue on Steganography, 2008. (Accepted for publication).
- [12] Umashankar Dewangan¹, Monisha Sharma², Swagata Bera³, "Wavelet Transform based Steganography" *International Journal of Advanced and Innovative Research (IJAIR)* ISSN: 2278-7844, 2012
- [13] H.C. Wu, N.I Wu, C.S. Tsai and M.S. Hwang, "Image Steganographic scheme based on pixel-value differencing and LSB replacement methods", *VISP(152)*, No. 5, October 2005
- [14] Cheng-Hsing Yang, Chi-Yao Weng, Shih-Jeng Wang, *Member, IEEE*, and Hung-Min Sun, "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 pp. 488-497.
- [15] Gurmeet Kaur and Aarti Kochhar, "Transform Domain Analysis of Image Steganography", *IJSETT International Journal for Science and Emerging Technologies with Latest Trends* 6(1), 29-37 (2013).
- [16] Barnali Gupta Banik, Samir Kumar Bandyopadhyay, "Implementation of Image Steganography Algorithm using Scrambled Image and Quantization Coefficient Modification in DCT" in *IEEE international conference on Research in computational intelligence and communication networks*.
- [17] Shahana T, "A Secure DCT Image Steganography based on Public-Key Cryptography" *International Journal of Computer Trends and Technology (IJCTT)* – volume 4 Issue 7–July 20
- [18] Hamad A. Al-Korbi¹, Ali Al-Ataby, Majid A. Al-Tae and Waleed Al-Nuaimy, "Highly efficient image steganography using Haar DWT for hiding miscellaneous data" *Jordanian Journal of Computers and Information Technology (JJCIT)*, Vol. 2, No. 1, April 2016.
- [19] Cheng Wei, Li Zhaodan, "Robust Watermarking Algorithm of Color Image Based on DWT-DCT and Chaotic System First IEEE International Conference on Computer Communication and the Internet 2016
- [20] Fengmei LIANG, Lijia WANG, "An Improve Wavelet-Based Color Image Watermark Algorithm," *Journal of Computational Information Systems* 7, vol. 6, pp. 2013-2020, 2011.

BIOGRAPHIES

	<p>Ms. Gurmeet Kaur received her M.Tech. degree in Electronics and Communication Engineering from DAVIET Jalandhar. Currently is working at CEC Landran as Assistant Professor in ECE Department . Her area of research includes Image Processing and Digital Signal Processing.</p>
	<p>Ms. Rasneet Kaur received her M.Tech. degree in CSE from Punjabi University , Patiala (Punjab). Currently is working at SUS , Tangori as Assistant Professor in CSE Department . Her area of research includes Wireless Sensor Networks.</p>
	<p>Ms. Amanpreet Kaur received her M.Sc.(Physics) degree from Punjab University, Chandigarh. M.Phil. from LPU Phagwara . Currently is working at CEC Landran as Assistant Professor in Applied Science Department.. Her area of research is Laser and Plasma.</p>
	<p>Ms. Harpreet Kaur received her M.Sc. degree in Physics . Currently is working at CEC Landran as Assistant Professor in Applied Science Department . Her area of research includes Optical Fibre Communication and Image Processing and Digital Signal Processing.</p>