International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Review on Different Methods of Image Steganography

Priyanka Dongardive[1], Neelesh Gupta[2], Meha Khare[3]

[1]M. Tech Research Scholar (EC), Truba Institute of Engineering and Information Technology, Bhopal

[2]Head of Department (EC), Truba Institute of Engineering and Information Technology, Bhopal

[3]Assistant Professor (EC), Truba Institute of Engineering and Information Technology, Bhopal

Abstract*: **Steganography is the specialty of concealing the way that correspondence is occurring, by concealing data in other data. Numerous distinctive transporter record organizations could be utilized; however computerized pictures are the most mainstream on account of their recurrence on the Internet. For concealing mystery data in pictures, there exists a vast assortment of steganography systems; some are more unpredictable than others and every one of them have particular solid and feeble focuses. Distinctive requisitions have diverse prerequisites of the steganography strategy utilized. Case in point, a few provisions may oblige outright imperceptibility of the mystery data, while others oblige a bigger mystery message to be covered up. In this paper we are contemplating the systems and strategies utilized for effective steganography. After investigation of different methods we can predict that the effective steganography could be structure with DCT and the clamor lessening for the recovery unknown data from stego picture.***

Keywords: Steganography, DWT, PSNR, JPEG image

1. Introduction

With the late developments in sight and sound interchanges and its impact in our electronic world, the essentialness of data security has been drastically expanded. Existing advances in the field of data security frameworks offer hiding the event of correspondence for anybody with the exception of the planned beneficiary. Thusly, steganography gives a solid answer for inserting discharge information into a spread media finely. Essentially, definitive targets of steganography are imperceptibility, heartiness, and high limit of the concealed information that separate it from related procedures, for example, watermarking and cryptography [17]. Likewise, the concealed message could be recuperated utilizing proper keys without any information of the first blanket media. All in all, steganography calculations normally battle with attaining a high implanting rate, expansive limit, and great intangibility.

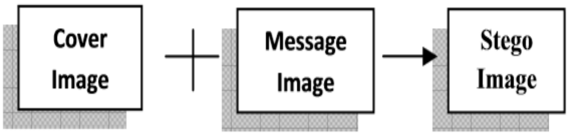


Figure 1: Steganography at sender's side

There are numerous provisions that make an effort the capability of steganography to conceal secrecy message as content, symbolism, or whatever available advanced indicator. Requisitions for such an information-concealing plan incorporate in-band inscribing, secret correspondence, picture sealing, correction following, upgrading strength of picture web indexes and savvy Ids (character cards) where distinctive points of interest are installed in their photos [17], [8].

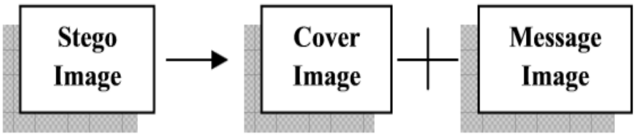


Figure 2: Steganography at receiver side

This work plans to present a proficient steganography method in picture records. The most widely recognized steganographic methods in advanced pictures concentrate on spatial space systems-which by and large utilize an immediate minimum huge bit (LSB) substitution method- and recurrence area techniques, for example, discrete cosine convert (DCT), Fourier change (FT), and discrete wavelet change (DWT). JPEG is an extremely famous picture arrangement, and it is additionally one of the primary bearers of data steganography engineering, so JPEG picture steganography identification has turned into one of the hot fields of data security. Steganography location is basically separated into specific steganography discovery and visually impaired steganography recognition, yet the recent is not for any particular picture steganographic calculations thus have a great adaptability. At present, the primary steganographic systems of JPEG picture are F5, MB (Model Based), Outguess, Steghide et cetera, and they practically altogether change the measurable properties in the DCT space of JPEG pictures. What's more, discrete wavelet convert (DWT) has been utilized in numerous reasonable steganographic systems due to its capability to fulfill fundamental concerns of data concealing framework, for example, limit and strength [10], [12]. Distinctive steganography plans have been proposed focused around Jpeg2000 coding framework which utilize discrete wavelet convert [14]. The progressive nature of the wavelet representation permits multiresolutional identification of the shrouded message, which is a Gaussian conveyed irregular vector added to all the high-pass groups in the wavelet area [10]. It is demonstrated that twisting came about because of pressure does not corrupt exact extraction of the relating shrouded message at every determination in the DWT area. A steganography strategy focused around breaking down both spread and mystery picture in wavelet space was exhibited by Abdelwahab et al. Each one deteriorated picture separated into 4×4 pieces and best match was dead set for each one squares of mystery picture which fit into the spread squares. Likewise, a DWT-based information concealing method was given by Banoci et al. in view of adjusting of wavelet coefficients [6]. Their trial outcomes showed that the proposed strategy attains great limit and proper picture quality.

2. Literature Review

Ashish Soni, Jitendra Jain, Rakesh Roshan [1], The Fractional Fourier Transform (Frft), as a generalization of the established Fourier convert, was presented numerous years back in arithmetic writing. For the upgraded calculation of partial Fourier convert, discrete adaptation of Frft started to be i.e. Dfrft. This paper delineates the preference of discrete fragmentary Fourier Transform (Dfrft) as contrasted with different converts for steganography in picture preparing. The reproduction outcome shows same PSNR in both area (time and recurrence) yet Dfrft gives preference of extra stego key i.e. request parameter of this change.

Nadeem Akhtar, Pragati Johri, Shahbaaz Khan[3], This work is concerned with executing Steganography for pictures, with a change in both security and picture quality. The particular case that is actualized here is a variety of plain LSB (Least Significant Bit) calculation. The stego-picture quality is enhanced by utilizing bit-reversal procedure. In this procedure, certain minimum huge bits of spread picture are upset after LSB steganography that co-happen with some example of different bits and that diminishes the amount of changed Lsbs. In this way, less number of minimum critical bits of spread picture is adjusted in correlation to plain LSB system, enhancing the PSNR of stego- picture. By putting away the bit designs for which LSBs are altered, message picture might be gotten accurately. To enhance the strength of steganography, Rc4 calculation has been utilized to attain the randomization sequestered from everything message picture bits into spread picture pixels as opposed to putting away them successively. This methodology haphazardly scatters the bits of the message in the spread picture and subsequently, making it harder for unapproved individuals to concentrate the first message. The proposed technique demonstrates great improvement to Least Significant Bit strategy in thought to security and in addition picture quality.

Jianyang, Shang-Ping zhong[3], Feature combination can successfully enhance the steganographic location proficience, however the past explores of characteristic combination in JPEG picture steganography identification once in a while recognized the nonlinear connection of characteristics. This paper examines the correspondence of JPEG picture steganographic characteristics and circuits characteristics with most reduced relationship to get better identification competence focused around KCCA (Kernel sanctioned connection investigation), which has a great capacity of nonlinear association dissection and can dispose of the repetition of data between characteristics. Firstly, break down the "DCT amplified characteristic" and the "markov diminished characteristic" which are fantastic characteristics, and the recently proposed "DCT versatile characteristic" in 2011. Besides, select two characteristics with least relationship around them for KCCA characteristic combination. At long last, complete trial appears differently in relation to other related strategies. The test effects demonstrate that the proposed system is sensible and powerful.

Table 1: Summary of Literature Review

Year	*Author*	*Title*	*Approach*	*Results*
2013	Ashish Soni, Jitendra Jain, Rakesh Roshan	Image Steganography using Discrete Fractional Fourier Transform	Fractional Fourier transform (FrFT), DFrFT	DFrFT gives an advantage of additional
2013	Nadeem Akhtar, Pragati Johri, Shahbaaz Khan	Enhancing the Security and Quality of LSB based Image Steganography	RC4 algorithm	Good enhancement to Least Significant Bit technique
2012	Jianyang, Shang-Ping zhong,	A JPEG Image Blind Steganography Detection Method Using Kcca Feature Fusion	KCCA (Kernel canonical correlation analysis),	Proposed method is reasonable and effective
2012	Hoda Motamedi, Ayyoob Jafari	A New Image Steganography Based on Denoising Methods in Wavelet Domain	Image denoising algorithms by wavelet thresholding	Excellent robustness against steganalysis attacks
2012	RigDas, Tuithung	A Novel Steganography Method for Image Based on Huffman Encoding	Image steganography based on Huffman Encoding	Algorithm has a high capacity and a good invisibility

Hoda Motamedi, Ayyoob Jafari[4], This paper presents a novel wavelet-based strategy to perform picture steganography using picture denoising calculations by wavelet thresholding. Steganographic calculations are when all is said in done focused around supplanting clamor parts of an advanced article with a to-be-shrouded message. The primary inspiration for leading this examination was to enhance strength and limit of shrouded information because of adequacy of wavelet change and intensity of loud parts as a fitting field for concealing mystery message. Indeed, mystery information is stowed away in uproarious segments of spread medium. Furthermore, the implanted information might be concentrated from the stego-picture without referencing the first picture and it has brilliant power against steganalysis ambushes.

Rigdas, Tuithung[5], This paper shows a novel method for picture steganography focused around Huffman Encoding. Two 8 bit ash level picture of size M X N and P X Q are utilized as spread picture and mystery picture individually.

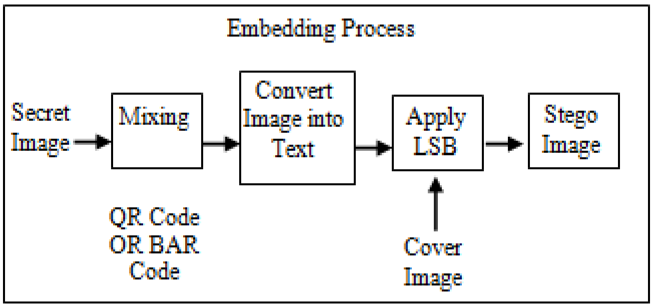
Huffman Encoding is performed over the mystery picture/message before implanting and every bit of Huffman code of mystery picture/message is implanted inside the spread picture by adjusting the slightest huge bit (LSB) of each of the pixel's intensities of spread picture. The trial consequence indicates that the calculation has a high limit and a great intangibility.

3. System Model

Steganography gives mystery of content or pictures to keep them from invaders. Steganography install the message picture in a spread picture and progressions its properties. Steganography gives mystery correspondence so that expected programmer or assailant unable to identify the vicinity of message. To keep the location of mystery messages is the significant craft of steganography. Steganography, determined from Greek, actually signifies "secured thinking of." It incorporates an immense exhibit of mystery specialized systems that cover the message's exceptionally presence. These strategies incorporate imperceptible inks, microdots, character game plan, computerized marks, clandestine channels, and spread range [7]. The essential idea is that it has a spread protest that is utilized to blanket the first message picture, a host question that is the message or principle picture which is to be transmitted, a stego-key which is utilized to conceal the message picture into spread picture, and the steganography calculation to complete the obliged item. The yield is a picture called stego-picture which has the message picture inside it, covered up. The preferences of Least-Significant-Bit (LSB) steganographic information implanting are that it is easy to see, simple to actualize, and it prepares stego-picture that is just about like spread picture and its visual unfaithfulness can't be judged by stripped eyes. A few steganography routines focused around LSB have been proposed and actualized [13][16][11].

A great strategy of picture steganography points at three perspectives. Initial one is limiting (the most extreme information that might be put away inside spread picture). Second one is the subtlety (the visual nature of stego-picture after information concealing) and the last is vigor [15]. The LSB based procedure is great at intangibility yet shrouded information limit is low on the grounds that stand out bit for every pixel is utilized for information covering up. Straightforward LSB strategy is additionally not strong on the grounds that mystery message might be recovered effortlessly once it is distinguished that the picture has some shrouded mystery information by recovering the LSBs.

4. Proposed Work



Multi layer encoding is adopted for the secret image by using bar code. Then the encoded secret image is converting into text. After that the text behind cover image is hidden. In this way enhancement is achieved for the security of secret image and improve the quality by increasing PSNR so that except sender or recipient no one can able to detect it.

5. Expected Result

After implementing the proposed methodology PSNR would be improved significantly than the previous work. In order to enhance the security of the image steganography the multi-stage encoding phenomena is adopted. In addition to this the overall complexity of the system will be decreased by implementing this approach.

6. Conclusion

In spite of the fact that just a percentage of the fundamental picture steganographic strategies were examined in this paper, one can see that there exists an expansive choice of methodologies to concealing data in pictures. All the significant picture document configurations have distinctive strategies for concealing messages, with diverse solid and frail focuses separately. Where one system needs in payload limit, alternate needs in strength. For instance, the patchwork approach has a large amount of vigor against most kind of strike, however can cover up just a little measure of data. Least noteworthy bit (LSB) in both BMP and GIF makes up for this, however both methodologies bring about suspicious records that expand the likelihood of discovery when in the vicinity of a warden.

References

[1] Ashish Soni, Jitendra Jain, Rakesh Roshan, "Image Steganography using Discrete Fractional Fourier Transform" 2013 International Conference on Intelligent Systems and Signal Processing (ISSP) 2013 IEEE.
[2] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan , "Enhancing the Security and Quality of LSB based Image Steganography" 2013 5th International Conference on Computational Intelligence and Communication Networks IEEE.
[3] Jianyang, Shang-Ping zhong, "A JPEG Image Blind Steganography Detection Method Using Kcca Feature Fusion", Proceedings ofthe2012 International Conference on Wavelet Analysis and PatternRecognition, Xian, 15-17July, 2012
[4] Hoda Motamedi, Ayyoob Jafari, "A New Image Steganography Based on Denoising Methods in Wavelet Domain" 2012 9th International ISC Conference on Information Security and Cryptology IEEE.
[5] RigDas, Tuithung, "A Novel Steganography Method for Image Based on Huffman Encoding" 2012 IEEE.
[6] V. Banoci, G. Bugar, D. Levicky, "A Novel Method of Image Steganography in DWT Domain," 21th International Conference on Radio elektronika, pp. 1-4, April 2011.

[7] Cheddad, J. Condell, K. Curran, & P. Kevitt, (2010). Digital image Steganography- survey and analysis of current methods. Signal Processing, 90, 727–752.

[8] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.

[9] L. Zhang, H. Wang, R. Wu, “A High-Capacity Steganography Scheme for JPEG2000 Baseline System,” IEEE Transactions on Image Processing, vol. 18, no.8, pp. 1797-1803, 2009.

[10] A. A. Abdelwahab, L. A. Hassan, “A discrete wavelet transform based technique for image data hiding,” Proceedings of 25th National Radio Science Conference, NRSC 2008, Egypt, pp. 1–9, March 18–20, 2008.

[11] D. Sandipan, A. Ajith, S. Sugata, An LSB Data Hiding Technique Using Prime Numbers, The Third International Symposium on Information Assurance and Security, Manchester, UK, IEEE CS press, 2007

[12] S. Liu, H. Yao, W. Gao, “Steganalysis of data hiding techniques in wavelet domain,” Proc. of Int. Conf. on Information Technology: Coding and Computing, pp. 751-754, 2004.

[13] C. K. Chan, L. M. Cheng, “Hiding data in image by simple LSB substitution”, pattern recognition, Vol. 37, No. 3, 2004, pp. 469-474.

[14] P. C. Su, C. C. J. Kuo, “Steganography in JPEG 2000 compressed images,” IEEE Trans. Consum. Electron., vol. 49, no. 4, pp. 824-832, 2003.

[15] C. Kessler. (2001). Steganography: Hiding Data within Data. An edited version of this paper with the title "Hiding Data in Data". Windows & .NET Magazine .http://www.garykessler.net/library/steganography.html

[16] R. Z. Wang, C. F. Lin and I. C. Lin, “Image Hiding by LSB substitution and genetic algorithm”, Pattern Recognition, Vol. 34, No. 3, pp. 671-683, 2001.

[17] L. M. Marvel, C. G. Boncelet Jr., and C. T. Retter, “Spread spectrum image steganography,” IEEE Trans. Image Process., vol. 8, no. 8, pp. 1075–1083, 1999.

[18] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Syst. J., vol. 35, 199