Performance Evaluation of Steganography Technique using SSIM

Arun Kumar Singh
Assistant Professor
AUH

Abstract-Todays in computerized world, PC serves to changing simple information into advanced shape before it can be put away or it can be preparing. For transmitting computerized information web is the most essential correspondence medium. In the event that any classified information to be transmitted over the web, at some point it is conceivable to duplicate, crush or roll out a few improvements in certain information by the vindictive client. To maintain a strategic distance from this different plans are as of late created. 0ne of the most imperative approach to conceal the safe data is the Steganography. It assumes a vital part to conceal the mystery data. In this plan installing an emit information into a cover message and sending it, message is any content, picture, sound/video record. The vast majority of the broadly utilized applications zone that utilizations steganography, for example, copyright insurance, web security, confirmation. In this paper propose another steganographic strategy for transmitting advanced pictures in light of discrete wavelet change utilizing two unique systems.

Keywords: Data hiding, Steganography, SSIM, DWT.

1. Introduction

Data hiding is the craftsmanship and investigation of undetectable communication. The word steganography is gotten from the Greek words ―stegos meaning ―cover and ―grafia meaning ―writing characterizing it as ―covered writing. In picture steganography the data is shrouded solely in pictures. There are a lot of difference between Steganography and cryptography as in where cryptography centers around keeping the substance of a message mystery, steganography centers around keeping the presence of a message mystery. Both approaches to shield data from undesirable gatherings however neither innovation alone is impeccable and can be imperiled. Once the nearness of shrouded data is uncovered or even suspected, the motivation behind steganography is incompletely vanquished. The quality of steganography would thus be able to be opened up by consolidating it with cryptography. These advancements are chiefly worried about the security of protected innovation; in this manner the calculations have unexpected prerequisites in comparison to steganography. These prerequisites of a decent steganographic calculation will be talked about underneath. In watermarking the majority of the cases of a question are ―marked similarly. The sort of data covered up in objects when utilizing watermarking is typically a mark to mean source or proprietorship with the end goal of copyright insurance. With fingerprinting then again, extraordinary, interesting imprints are inserted in unmistakable duplicates of the bearer question that are provided to various clients. This empowers the protected innovation proprietor to recognize clients who break their permitting assertion by providing the property to outsiders.

2. Literature Review

This paper plans to watch the impact of implanting the mystery message in various groups, for example, CH, CV and CD on the execution of stego picture as far as Peak Signal to Noise Ratio (PSNR). Experimentation has been finished utilizing six unique assaults. Trial comes about uncover that the mistake square supplanting with slanting point of interest coefficients (CD) gives preferable PSNR over doing as such with different coefficients. [3]

The picture is changed over into recurrence space in the wake of applying wavelet change. The cover picture is changed over from RGB to Gray scale which is more appropriate organization for information stowing away. The mystery message or picture which is to cover up is at that point handled to know the measure of that mystery message or picture. A key is utilized to give mystery which creates the PN grouping for concealing mystery message in cover picture. Apply reasonable calculation for concealing the message. The mystery message is being covered up at the edges of the cover picture. PSNR is figured by applying scientific activity. [4]

This paper displays the utilization of Wavelet Transform and Genetic Algorithm in a novel steganography plot. We utilize a hereditary calculation based mapping capacity to install information in DWT coefficients in 4*4 squares on the cover picture. The ideal pixel modification process is connected in the wake of installing the message. We use the recurrence space to enhance the power of steganography and, we execute Genetic Algorithm and Optimal Pixel Adjustment Process to acquire an ideal mapping capacity to lessen the distinction blunder between the stego-picture and the cover image, along these lines enhancing the concealing limit with low twists. Our Simulation comes about uncover that the novel plan beats versatile steganography system in light of wavelet change as far as pinnacle flag to commotion proportion and limit, 39.94 dB. [5]

3. The proposed method

Algorithm for Data Hiding

1. Select given secret image and cover image
2. Compress secret message and take 2D DWT of the cover image

3. Calculate scaling factor (secret key)
4. Perform Hiding process

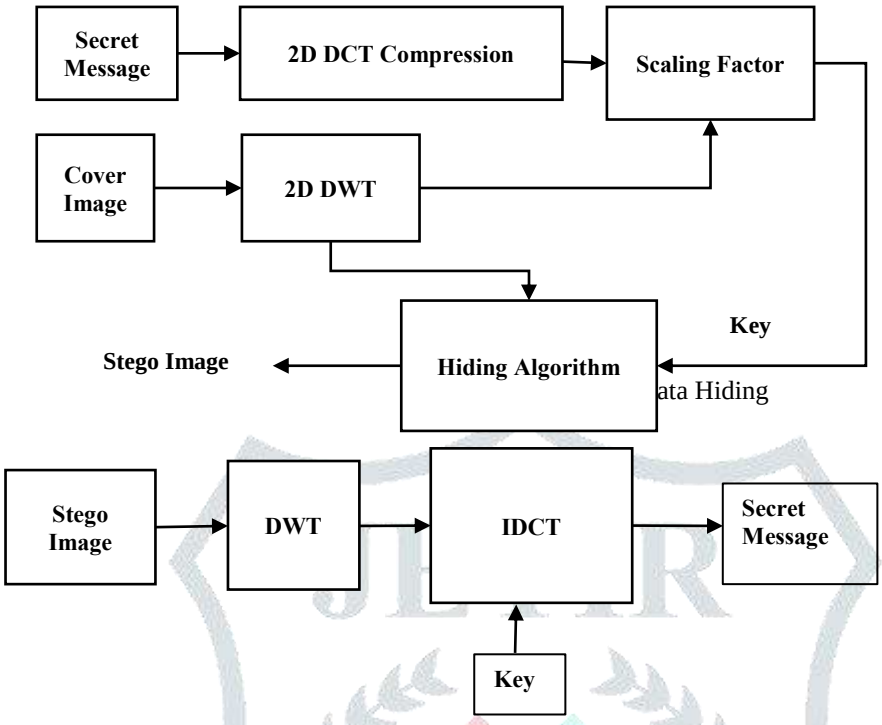

Fig. 5. Algorithm for Data Extraction

Fig3: Original Cover Image Taken for Data Hiding

Algorithm for Data Extraction

1. Select stego image and take 2D DWT
2. Extract DCT coefficient from above matrix
3. Take IDCT transform to generate secret image

Fig4: Stego Image After Data Hiding

4. Noise Analysis and Experimental Result

The structural similarity (*SSIM*) index

The SSIM is a notable quality metric used to quantify the comparability between two pictures. It is thought to be related with the quality view of the human visual framework (HVS). Rather than utilizing conventional blunder summation strategies, the SSIM is planned by demonstrating any picture twisting as a blend of three factors that are loss of connection, luminance bending and complexity mutilation. The SSIM is characterized as:

The Structural Similarity (SSIM) Index quality evaluation list depends on the calculation of three terms, luminance(l), contrast (c) and structure (s). The general formula to calculate SSIM given below as [1]

$$SSIM\ (x, y) = [l(x, y)]^{\alpha} \cdot [c(x, y)]^{\beta} \cdot [s(x, y)]^{\gamma}$$

where

$$\mathbf{l(x,y)}=\frac{2\mu_x\mu_y+c_1}{\mu_x^2+\mu_y^2+c_1}$$

$$\boldsymbol{c(x,y)}=\frac{2\delta_x\delta_y+c_2}{\delta_x^2+\delta_y^2+c_2}$$

$$\boldsymbol{s(x,y)}=\frac{\delta_{xy}+c_3}{\delta_x\delta_y+c_3}$$

where μ_x, μ_y, σ_x, σ_y, and σ_{xy} are the average, SD, and cross-covariance for images. If $\alpha = \beta = \gamma = 1$ (default), and $C_3 = C_2/2$ (default) the index simplifies to:

$$\boldsymbol{SSIM(x,y)}=\frac{(2\mu_x\mu_y+c_1)}{(\mu_x^2+\mu_y^2+c_1)}\frac{(2\delta_x\delta_y+c_2)}{(\delta_x^2+\delta_y^2+c_2)}$$

There are no exact tenets for choosing the SSIM or the PSNR when the assessment of picture quality is required. Subsequently, casual contentions and conviction direct the understanding of numerical qualities got amid the assessment procedure. Actually, a few investigations have uncovered that rather than the SSIM, the MSE thus the PSNR perform gravely in segregating basic substance in pictures since different sorts of corruptions connected to a similar picture can yield a similar estimation of the MSE. Different examinations have demonstrated that the MSE, and therefore the PSNR, have the best execution in evaluating the nature of uproarious pictures. [2]

S. No.	Cover Image	SSIM
1	CoverImage1	0.984980302051827
2	CoverImage2	0.979474526814775
3	CoverImage3	0.998084597993745
4	CoverImage4	0.969544351465274
5	CoverImage5	0.996677162187304
6	CoverImage6	0.997174252479752
7	CoverImage7	0.988806752354798

Conclusions

In this technique SSIM is being used as quality measurement parameter. The result in the above table proves that the proposed method is very much effective in data hiding technique. Maximum value of SSIM should be 1 and in above table all values are near to one.

References

[1] http://in.mathworks.com/help/images/ref/ssim.html
[2] Alain Horé, "Image quality metrics: PSNR vs. SSIM", 2010 IEEE International Conference on Pattern Recognition, pp2366.
[3] Vijay Kumar, "Performance Evaluation of DWT Based Image Steganography", *2010 IEEE 2nd International Advance Computing Conference*
[4] Dr. MAHESH KUMAR, "Image Steganography Using Frequency Domain" INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 3, ISSUE 9, SEPTEMBER 2014.
[5]Elham Ghasemi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm" ,IMECS 2011 Vol-1.