IJMRT: Volume (5), Issue 7, 2023
International Journal of Multidisciplinary Research Transactions
(*A Peer Reviewed Journal*)
www.ijmrt.in

ISSN (Print):2663-2381
ISSN(Online):2663-4007

Secured Data Transmission Scheme using Discrete Wavelet Transform Decomposition for Still Images

Hariprasath. S[1], Giri Rajkumar. S.M[2], Ratnagirish. R. K[3], Shyam Prakash. G. P[4], Surya. M[5*]

[1]*Assistant Professor, Department of Electronics and Communication Engineering, Saranathan College of Engineering, India.*
[2] *Professor, Department of Instrumentation and Control Engineering, Saranathan College of Engineering, India.*
[3,4,5]*Student, Department of Instrumentation and Control Engineering, Saranathan College of Engineering, India.*

[*]Corresponding author

DoI: https://doi.org/10.5281/zenodo.7921806

Abstract

Secured transmission of information over the unreliable wireless channel is a profound research work in the field of wireless communication. In spite of the availability of various algorithms and their implementations, yet there is a need for improved methods of transfer of information. Steganography is one such technique through which secured data transfer is made possible. By hiding the highly sensitive information in embedding inside the cover image, using image steganography information sharing is authenticated. In this work, the cover image is decomposed and proper sub image is chosen using discrete wavelet packet transform and the sensitive information is hidden at the transmitter section. The wireless channel behavior is mimicked by introducing noises and the detection and recovery of the hidden information at the receiver is carried out. The performance is analyzed with standard metrics like Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The PSNR achieved is 92.5% which is sufficient enough for image steganography techniques. By incorporating transform based techniques other than DWT, the performance could be improved.

Keywords: Wireless, Steganography.

1. Introduction

Steganography, which is defined as covered writing, is derived from the Greek word steganos, where stego stands for cover and grafia for writing. The right information must be communicated at the appropriate time and exclusively to the intended audience. Information is a valuable asset that has to be protected from theft and alteration. The sharing and preservation of personal information is made difficult by the constantly changing danger environment, which is supported by effective attack vectors. The amount of security vulnerabilities is growing, and handling this sensitive information by illiterate or ignorant handlers can be challenging. Steganography is utilized to hide sensitive information by embedding it in a Cover Image (CI) in order to secure authentic information. While information is being transmitted via the internet. Steganography is a way of safeguarding hidden information in carriers like a video, audio, digitalimage, or text that is used to protect online privacy. Image steganography, or the incorporation ofsensitive information into the CI through pixel value changes, creates a stego-image.

A. Contribution: Beta blending based image steganography using DWT is proposed in this work.

B. Organization: Section 2 describes existing systems; Section 3 details the proposed method. Sections 4 explain results and section 5 provides conclusion and future scope.

2. Existing Idea

Aya Jaradat et al. [1] suggested an optimization based on Particle Swarm Optimization as a method for locating the ideal pixel location in the cover image to mask the payload image. An improved version of the Least Significant Bit (LSB) was suggested by Mansoor Fateh et al. [2]. Two bits of the payload are placed in two CI pixels once the payload is transformed into a bit-stream. In the method introduced by J. B. Eseyin and K. A. Gbola-Gade[3], Information

protection based on the Residue Number System (RNS), Chinese Remainder Theorem (CRT), and encryption using the RSA method were discussed in detail.

One of the most effective adaptive patterns, enhances the inverted LSB's embedding performance according the method proposed by Supriadi Rustad et al. [4]. In the method proposed by Nabanita Mukherjee (Ganguly) et al. [5], the method of hiding a byte of data is explained in detail. Genetic Algorithm (GA) based method was proposed by Pratik D. Shah and Rajankumar S. Bichkar [6] to modify the payload and embedding in the LSBs of the cover image. For image steganography, Atta R et al.[7] suggested the Advanced Exploiting Modification Direction (AEMD).

To boost concealing capacity, edge pixels have more bits buried than non-edge pixels. Using adaptive LSB, Abdel Raouf and Ashraf [8] devised an information-hiding method based on the human visual system. Color image steganography employing an adaptive fuzzy inference as a classifier and LSB was proposed by Tang L et al.[9]. Huffman Encoding (HE) and PSO were suggested as an image steganography technique by Sharma N. and Usha Batra [10]. A color image steganography for the wireless medium was suggested by Asmaa A. E. et al. [11]. The Discrete Cosine Transform (DCT) and DWT are the foundation of the method used in this work.

Image steganography utilizing LSB and PVD was proposed by Aditya Kumar Sahu and Gandharba Swain [12]. A Pixel-based Adaptive Directional Pixel Value Differencing (P-ADPVD) approach for image steganography was proposed by M. Hassaballah et al [13]. Payload is hidden using the Pixel-of-Interest (POI) technique. The identification of people using biometric traits was proposed by Douglas, Bailey, Leeney, and Curran [14]. To increase security, image steganography is employed. A painting-assisted reversible steganography using

a histogram shifting technique and partial differential equations (PDE) for embedding was proposed by Chuan Qinet et al. [15].

The BCH equations were proposed by Rongyue Zhang et al [16].(BCH)code for steganography. For large capacity and security, H S Manjunatha Reddy and K B Raja[17] recommended empl oying DWT image steganography.

3. Proposed System

The proposed model of image steganography based DWT using alpha blending technique for secure communication is as shown in the above flow chart Cover Image (CI): Describes the medium that conceals the secret information. We employ prepared photos of various types, live webcam images, and cover images of various dimensions. i.e., black-and-white and color photos. The original information to be transmitted is referred to as the payload image (PI). It uses a payload picture with various size and formats. Normalization is the division of all CI and PI pixels into groups of pixels with the highest possible value. Pre-processing: In pre-processing, scaling operations are carried out. All of the CI and PI pixels in this work are multiplied by the strength factors and, respectively.

Beta Blending: Beta blending is given by

$$SI = \alpha * CI + \beta * PI \quad - (1)$$

Where $\beta = (1- \alpha)$, SI is Stego image and α, βare the strength scaling factors

3.1. Discrete Wavelet Transformation (DWT)

Discrete Wavelet Transforms is a powerful signal representation tool. When DWT is applied to the image, first the High-Pass Filter (H) and the Low-Pass Filter (L) are used for each row, and then they are down-sampled by 2 to get the row's high-and low-frequency information. Later,

H and L filters are applied again for each high-and low-frequency column component, and then they are down-sampled by 2. The four sub-bands generated are, i.e., the LL, HL, LH, and HH bands. The complete information is available in the LL-band at the third level for implementation, the two-dimensional DWT is used.

In this case, where the 2 ×2 Haar transform (H2) equation is considered to maintain the regional details, which is given by Eq. (2) as,

H 2 = 1 √2 [1 1 1 −1] ×[**a b c d**] Where, a, b, c and d →2 ×2 input image sub-matrix. Similarly, to get IDWT the transpose of the input matrix presents in Eq. (2) is used. The retrieval of the payload image is as shown in Fig. 2

3.2. Stego Image Generation Algorithm

Step A: Initialize $\alpha$and βstrength factors; where β= (1- α)

Step B: Read CI and resize it to 256 ×256; read PI and resize it to 512 ×512.

Step C: Normalize Cover Image (NCI) = CI/255 and Normalize Pay- load Image (NPI) = PI/255

Step D: Preprocessing Cover Image (PCI) = (NCI) ∗ $\alpha$and Preprocessing Payload Image (PPI) = (NPI ∗ β).

Step E: Apply 2D DWT wavelet on CI and PI and choose the LL band of CI and PI, respectively.

Step F: Encryption-Square and add the LL band coefficient of CI and PI and then apply the DWT.

Step G: Embedding the payload in CI to generate a Stego Image (SI), i.e., LL, LH, HL, HH bands of encrypted PI are embedded in respective bands of the CI using fusion, and Inverse Discrete Wavelet Transform (IDWT) is applied to generate SI.

3.3. Secret Image Extraction Algorithm

Step A: Read the SI.

Step B: (i) Apply the 2D-DWT wavelet on SI to get the sub-bands. (ii) Subtraction of SI coefficients from CI coefficients (iii) Apply IDWT

Step C: Decryption-Take the square root of the previous step, divide by two, and divide by β.

Step D: The image obtained in step3 is multiplied by 255, and the payload is retrieved.

4. Results and Discussion

Mean Square Error (MSE): MSE is a metric used to quantify visual distortion [40, 41].

Equation (3) is used to calculate the sum of the square of the error between SI and CI.

$$\mathbf{MSE} = [1\ \mathbf{R} *]\ \Sigma\mathbf{i} = 1\ \mathbf{N}\ \Sigma\mathbf{j} = 1\ (\ \mathbf{SI} - \mathbf{CI}\ )\ 2 \text{ -(3)}$$

CI stands for cover image pixels. Stego picture pixels are SI. The dimension of the image is represented as R C, where R is row and C is column.

PSNR, or Peak Signal to Noise Ratio PSNR, which measures the quality of the image by comparing SI and CI, is the statistical difference between SI and CI [42]. It is provided by Eq. (4) and measured in dB.

$$\mathbf{PSNR} = 20\ \mathbf{log}\ [\ (2\ \mathbf{k} - 1\ )\sqrt{\mathbf{MSE}}\ ]$$ k is the amount of bits needed to represent a pixel in an 8-bit grayscale image, where (4).

Eq. (5) provides PSNR.

$$\mathbf{PSNR} = 20\ \mathbf{log}\ [\ 255\ \sqrt{\mathbf{MSE}}\ ]$$ Entropy(N) is the intensity value state to which each pixel adjusts. $$\mathbf{N} = -\ \mathbf{n} - 1\ \Sigma\mathbf{i} = 0\ \mathbf{n} - 1\ \Sigma\mathbf{j} = 0\ \mathbf{p}\ (\ ,\ \mathbf{j}\ )\ \mathbf{lo\ g\ b}\ \mathbf{p}\ (\ \mathbf{i}\ ,\ \mathbf{j}\ )$$ - (6) The result is given in bits where p holds the normalised histogram counts and n is the quantity of grayscale values. Table 1 represents PSNR value for various values of a for a CI and PI.

Table.1. PSNR value for a CI and PI for various values of a.

α	CI	PI	MSE	PSNR	N1	N2
0.9	circuit	lena	0.1401	65.2003	2.9163	2.9163
0.8	circuit	lena	0.1402	65.1969	2.9167	2.9163
0.4	circuit	lena	0.1404	65.1837	2.9149	2.9163
0.1	circuit	lena	0.1406	65.1740	2.7843	2.9163

Table 1 displays the experimentation with CI and PI of dimension 512 512 with values ranging from 0.1 to 0.999. MSE and PSNR are 0.1406 and 65.1740 for = 0.1 and 0.401 and 65.2036 for = 0.999, respectively.

Table.2. PSNR value for color CI and grayscale PI

A	**CI**	**Dimension**	**PI**	**Dimension**	**MSE**	**PSNR**	**NI**	**N2**
0.9	peppers.png	512x512	airplane.png	512x512	0.7315	50.8455	3.1695	3.1676
0.9	airplane.png	512x512	Peppers.png	512x512	0.5447	53.4071	2.5050	2.5050

The PSNR values for colour CI and grayscale PI are displayed in Table 2. Baboon's colour image serves as the control, and Barbara's grayscale image is used for testing at =0.999. The entropy of stego and the cover picture are 2.9163 and 2.9163, respectively, and the PSNR obtained is 65.2036, with an MSE of 0.1401.

Table. 3. PSNR value for grayscale and color PI

A	**CI**	**Dimension**	**PI**	**Dimension**	**MSE**	**PSNR**	**NI**	**N2**
0.9	rice.png	512x512	lena.png	512x512	0.3035	58.4878	3.1097	3.1097
0.9	lena.png	512x512	rice.png	512x512	0.2140	61.5224	3.0553	3.0562

The PSNR values for CI as a grayscale image and PI as a colour image are displayed in Table 3. Lena's colour image and Goldhill's grayscale image are used for testing at =0.999. The

stego and cover images' entropies are 3.0553 and 3.0562, respectively, and the PSNR obtained is 661.5224, with an MSE of 0.2140.

Table.4. PSNR value for various CI and PI grayscale images

A	Image	Dimension	Image	Dimension	MSE	PSNR	N1	N2
0.9	cameraman.tif	512x512	baboon.jpg	256x256	0.2685	59.5527	3.0845	3.0845
0.9	baboon.jpg	512x512	Cameraman.tif	256x256	0.2179	61.3659	3.0554	3.0561

The grayscale CI and PI's PSNR value is displayed in Table 4. For testing, the grayscale pictures rice.png are used as the control image (CI), and testpat1.png is used as the input image (PI). The MSE is 0. 0.1634, the PSNR obtained is 63.8647, and the entropies of the stego and cover images are 3.0765 and 3.0713, respectively.

Table. 5. PSNR value for color CI and PI

A	Image	Dimension	Image	Dimension	MSE	PSNR	N1	N2
0.9	lena.png	512x512	circuit.tif	256x256	0.4163	55.7420	3.0713	3.0713
0.9	circuit.tif	512x512	lena.png	256x256	0.1907	62.528	2.8729	2.8732

The PSNR values for the colours CI and PI are displayed in Table 5. The onion.png is used as the PI and peppers.png is used as the CI for testing at =0.999. The MSE is 0.1206 and the entropy of the stego and cover images are 2.5015 and 2.5015, respectively, with a PSNR of 66.5025.

6. Conclusion

MATLAB is used to create the suggested method for image steganography for performance analysis using an alpha blending-based Haar DWT for secure communication. A stego picture is created when the payload image is embedded into the CI. The predefined grayscale, colour

pictures from the database, and live images are all taken into consideration in this work for experimentation in various dimensions. The recovered secret and stego images' result parameter, or PSNR, is high, showing that there isn't much of a distinction between them and the transmitted images.

Table 2 shows the PSNR value of grayscale CI and color PI. The grayscale image of Baboon as CI and color image PI as Barbara, the PSNR obtained is 65.2036, MSE is 0.1401. Table 3 shows the PSNR value of CI as a grayscale image and PI as a color image. The grayscale image Goldhill as CI and the color image Lena, the PSNR obtained is 61.5224, and the MSE is 0.2140. Table 4 shows the PSNR value of the grayscale CI and PI. The grayscale image rice as CI and testpat1 as PI, the PSNR obtained is 63.8647, and the MSE is 0.1632. Table 5 shows the PSNR value for the colors CI and PI. With the pepper as CI and the onion as PI, the PSNR obtained is 66.5025, and the MSE is 0.1206.

REFERENCES

[1]. Aya Jaradat, Eyad Taqieddin, Moad Mowafi, A high-capacity image steganography method using chaotic particle swarm optimization, Secur. Commun. Netw. 2021 (2021) Article ID 6679284.

[2]. Mansoor Fateh, Mohsen Rezvani, Yasser Irani, A new method of coding for steganog- raphy based on LSB matching revisited, Secur. Commun. Netw. 2021 (2021) Article ID 6610678.

[3]. J.B. Eseyin, K.A. Gbolagade, Data hiding in digital image for efficient information safety based on residue number system, AJRCoS 8 (4) (2021) 35–44.

[4]. Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur, Pulung Nurtan- tio Andono, Inverted LSB image steganography using adaptive pattern to improve imperceptibility, J. King Saud Univ. Comput.Inf. Sci. (2021) ISSN 1319-1578.

[5]. Nabanita Mukherjee (Ganguly), Goutam Paul, Sanjoy Kumar Saha, Two-point FFT-based high capacity image steganography using calendar based message en- coding, Inf. Sci. 552 (2021) 278–290 ISSN 0020-0255.

[6]. Pratik D.Shah, Rajankumar S Bichkar, Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure, Eng. Sci. Technol. Int. J. 24 (3) (2021) 782–794 ISSN 2215-0986.

[7]. R. Atta, M. Ghanbari, I. Elnahry, Advanced image steganography based on exploit- ing modification direction and neutrosophic set, Multimedia Tools Appl. (2021) 21751–21769.

[8]. Ashraf Abdel Raouf, A new data hiding approach for image steganography based on visual color sensitivity, Multimedia Tools Appl. (2021) 23393–23417.

[9]. L. Tang, D. Wu, H. Wang, et al., An adaptive fuzzy inference approach for color image steganography, Appl. Soft Comput. (2021) 10987–11004.

[10]. N. Sharma, Usha Batra, An enhanced Huffman-PSO based image optimization al- gorithm for image steganography, Genetic Programm. Evolvable Mach. (2021), 189–205.
[11]. Aditya Kumar Sahu, Gandharba Swain, An improved method for high hiding capac- ity based on LSB and PVD, in: Digital Media Steganography, Academic Press, 2020, pp. 41–64. ISBN 9780128194386.
[12]. M. Hassaballah, Mohamed Abdel Hameed, Saleh Aly, A.S. AbdelRady, A color image steganography method based on ADPVD and HOG techniques, in: Digital Media Steganography, Academic Press, 2020, pp. 17–40. ISBN 9780128194386.
[13]. M. Douglas, K. Bailey, M. Leeney, K. Curran, An overview of steganography tech- niques applied to the protection of biometric data, Multimedia Tools Appl. (2017)17333–17373.
[14]. Chuan Qin, Chin-Chen Chang, Ying-Hsuan Huang, Li-Ting Liao, An inpainting-as- sisted reversible steganographic scheme using a histogram shifting mechanism, IEEE Trans. Circuits Syst. Video Technol. 23 (7) (2013) 1109–1118.
[15]. Rongyue Zhang, Vasiliy Sachnev, Magnus Bakke Botnan, Hyoung Joong Kim, Jun Heo, An efficient embedder for BCH coding for steganography, IEEE Trans. Inf. Theory 58 (12) (2012) 7272–7279.
[16]. H.S. Majunatha Reddy, K.B. Raja, High capacity and security steganography using discrete wavelet transform, Int. J. Comput. Sci. Secur. (IJCSS) 3 (6) (2012) 462–472.