A Novel Steganographic Scheme Using Weighted Matrix in Transform Domain

Partha Chowdhuri[1(✉)], Biswapati Jana[1], and Debasis Giri[2]

[1] Department of Computer Science, Vidyasagar University, Midnapore 721102, West Bengal, India
prc.email@gmail.com, biswapatijana@gmail.com

[2] Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia 721657, West Bengal, India
debasis_giri@hotmail.com

Abstract. In this paper a weighted matrix based steganographic scheme has been developed based on Discrete Cosine Transform (DCT). First, (8×8) quantized DCT coefficient blocks are obtained from the cover image. Instead of hiding the data directory to the quantized DCT coefficient blocks, a different approach has been taken here. The AC coefficients, except 0 coefficients, are used to form a series of 3×3 temporary matrices. Then, each four bits secret data is converted into an integer value. An user defined weighted matrix is used to select the position in the temporary matrix where the data will be embedded. The integer value is then embedded into that particular position of the selected temporary matrix. The proposed method is tested using different steganographic attacks like RS analysis and NCC to show that the scheme is undetectable under these analysis and more robust that other schemes. This scheme provides good embedding capacity with high visual quality of stego images.

Keywords: Steganography · Weighted matrix
Quantized DCT coefficient · PSNR · NCC

1 Introduction

Due to the rapid development of computer technology and Internet, hiding data within the digital format of multimedia became very popular. Many schemes for hiding data have been proposed till date. These approaches are classified mainly into two categories: the spatial-domain and the frequency-domain. In spatial domain, the pixel values are directly manipulated to hide data. Noticeable distortion in any position of the image is a common case in spatial domain. Therefore, different approaches have been developed to increase the embedding capacity and to adjust the position to minimise the distortion noticeable to human eye. Some inherent problem of spatial-domain data hiding is there. For an example, for lossy compression it is very difficult to find the redundant portion of the

D. Ghosh et al. (Eds.): ICMC 2018, CCIS 834, pp. 27–35, 2018.
https://doi.org/10.1007/978-981-13-0023-3_3

image for hiding data. But this redundant portion can be easily detected when we transform the image to frequency domain. The sharp transitions and edges of an image contribute the high-frequency content to its discrete cosine transform. Thus, to find the appropriate pixels to hide the data, transform domain scheme is a better approach. In transform domain schemes, some frequency oriented mechanisms like Discrete Cosine Transform (DCT) is used to transform the cover image. The secret data are then embedded into the cover image by modifying the frequency coefficients.

The Joint Photographic Experts Group (JPEG) digital image format is most popularly used image format nowadays. But, as JPEG is a compressed image format and uses transform domain principles, a slight modification in the transform domain may cause more distortion to the cover image. Most of the existing steganographic schemes changes one coefficient for hiding one bit of data. So, hiding more data causes changing more coefficients that gradually degrade the quality of the cover image which makes it prone to suspicion. We have used weighted matrix for our scheme to embed more data by changing one DCT coefficient. This increases the robustness as well as the quality of the image.

The remainder of the paper is constructed as follows: In Sect. 2 Motivation and objectives of our proposed techniques is described. In Sect. 3 the proposed scheme is presented. Experimental results and comparisons are shown in Sect. 4. In Sect. 5 Steganalysis and evolution are discussed Finally conclusions are depicted in Sect. 6.

2 Motivation and Objective

The main motivation and objective of the proposed work are listed below:

(i) Embedding Capacity: In the literature, it is observed that payload is limited when using weighted matrix in the steganographic scheme. So our motivation is to increase data embedding capacity.

(ii) Imperceptibility: It is well known that imperceptibility is the main requirement in any steganographic scheme. So first and foremost objective is to maintain imperceptibility in the proposed scheme.

(iii) Robustness: From the literature, it is seen that till now there exist some security loop hole in any steganographic scheme in real life. So our objective is to develop a steganographic scheme using weighted matrix through predefined integer sequence to enhance security and robustness.

3 Proposed Method

In this section, we proposed a novel data hiding technique based on discrete cosine transformation (DCT) using weighted matrix. We first transform a given cover image into a sequence of 8×8 blocks of DCT coefficients. The schematic diagram of secret data embedding and extraction are depicted in Figs. 1 and 2 respectively.

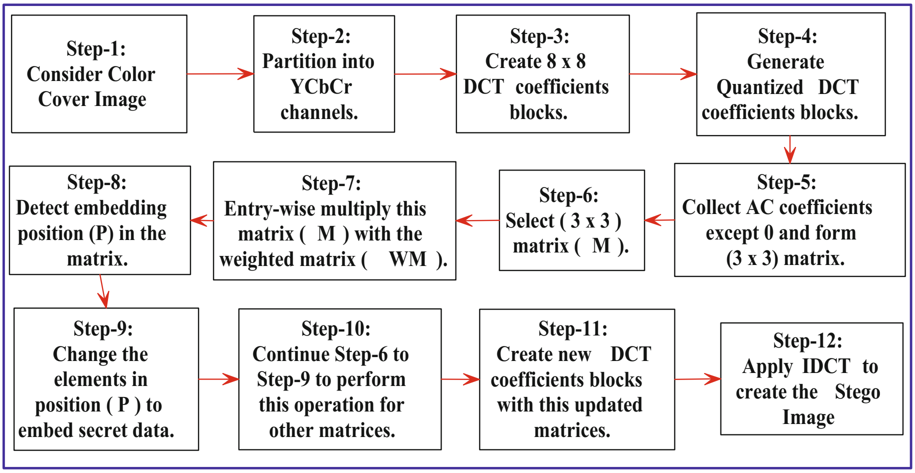

Fig. 1. Details of embedding process

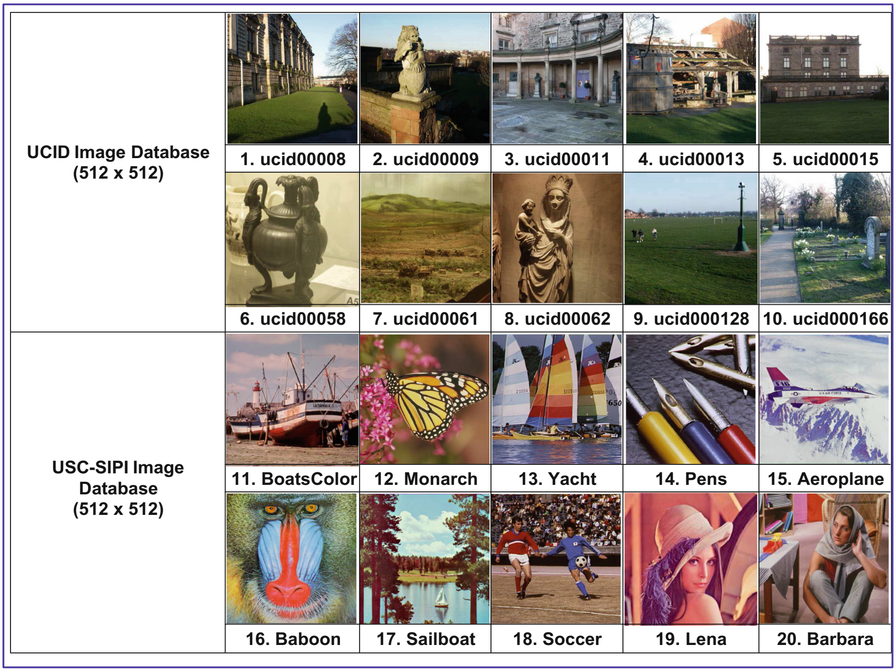

Fig. 2. Cover images with (512 $\times$ 512) pixel collected from the standard benchmark databases like UCID and USC-SIPI

3.1 Embedding Phase

The embedding technique can be explained by the following steps:

(1) Take the original cover image $CI_{m \times n}$ and secret image (SI) as input.
(2) Now to create DCT coefficient matrices DCT is applied to all 8×8 image blocks of the $CI_{m \times n}$. Then Quantized DCT is obtained from the DCT coefficient matrix.
(3) The AC coefficients, except 0 coefficients, from the DCT coefficient matrices are taken to form a series of 3×3 Temporary Matrices (TM) for embedding secret data.
(4) The secret image (SI) is also converted to binary form to create binary secret message (SM).
(5) First, a Temporary Matrix (TM) is taken for processing.
(6) 4 bits data is taken from the secret message (SM) and then converted to its equivalent decimal value (DV).
(7) Elementary multiplication is done between the Temporary Matrix (TM) and the weighted matrix (WM).
(8) The embedding position in the Temporary Matrix (TM) is selected using the standard weight matrix rule.
(9) The decimal value (DV) is embedded into the particular position in Temporary Matrix (TM).
(10) Step 5 to Step 9 is applied for the rest of the Temporary Matrices (TM).
(11) The quantized DCT block coefficients are updated using the Temporary Matrices (TM).
(12) Inverse DCT is applied to all the quantized DCT blocks to form the YCbCr channels.
(13) Finally, using the YCbCr channels, the stego image is created.

3.2 Extraction Phase

The extraction technique can be explained with the following steps:

(1) Take the stego image $SI_{m \times n}$ and secret Weighted Matrix (3×3) as input.
(2) Now DCT is applied in all 8×8 image blocks of the $SI_{m \times n}$ to get the DCT coefficients. Then Quantized DCT is obtained.
(3) Temporary Matrices ($TM_{3 \times 3}$) are created from the AC coefficients (except 0 coefficient).
(4) Now 4 bit secret data is extracted from Temporary Matrix (TM) by applying entry-wise multiplication with the weighted matrix (WM).
(5) This process is done with all other Temporary Matrices to extract all 4 bit data.
(6) All 4 bit data, extracted from all the Temporary Matrices, are concatenated to form the secret binary bits.
(7) The original secret image is generated from this secret binary bits.

4 Experimental Results and Comparisons

The proposed method is discussed in this paper is implemented in Java 9 windows 10 (operating system) environment. The computational platform was a Intel Core i5-6200U processor with a speed of 2.40 GHz and 4 GB RAM. A set of standard colour test images with size (512×512) are chosen to evaluate the performance of the proposed scheme. Figure 2 shows some of the standard colour test images which were collected form "USC-SIPI" image database [9] collected from the University of Southern California, "UCID" image dataset [5] consist of 1338 uncompressed color image collected from the Nottingham Trent University, UK. We have used secret message as logo image of size (54×54). The performance evaluation of the proposed scheme is evaluated using Mean Square Error (MSE), Peak-Signal-to- Noise-Ratio $(PSNR)$ Normalized Cross Correlation (NCC) and Structural similarity $(SSIM)$ index.

The imperceptibility of the stego image from the original image is indicated by the PSNR defined as:

$$MSE = \frac{\sum_{i=1}^{Row} \sum_{j=1}^{Col} [X(i,j) - Y(i,j)]^2}{(Row \times Col)} \tag{1}$$

$$PSNR = 10\ log_{20} \frac{I_{max}}{MSE} dB \tag{2}$$

Table 1. Comparison of proposed scheme with Chang et al. and Weng et al's scheme in terms of visual quality (PSNR).

Image	Chang et al. [1]		Weng et al. [11]		Proposed scheme	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	12288	35.15	28.364	42.42	36864	49.92
Baboon	12288	31.34	6708	48.17	36864	47.25
Airplane	12288	35.22	27694	45.73	36864	46.33
Boat	12288	34.92	15564	45.72	36864	47.25
Zelda	12288	38.04	22504	43.05	36864	46.89
Pepper	12288	36.32	20191	48.15	36864	46.92
Average	12288	35.17	20170	45.54	36864	47.37

where Row and Col is the size of cover image $(X(i,j))$ and stego image $(Y(i,j))$. Where I_{max} is the peak signal value of the cover image which is equal to 255 for 8 bit images. High PSNR value assure better image quality and low PSNR implies poor image quality. Table 1 represent the experimental value of average PSNR which is greater than 47 dB and the maximum embedding capacity is $= 36,864$ bits. The bpp in this scheme $= \frac{Total\ embedded\ bits}{(Row \times Col)} = 0.14$. Structural similarity (SSIM) index is a parameter for measuring the similarity between two images. Its value lies between −1 and +1. Its value approaches to +1 when two images are identical. The following formula is used to find the SSIM value of the Cover and Stego images.

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{3}$$

where, μ_x is the average of x, μ_y is the average of y;
${\sigma^2}_x$ is the variance of x, ${\sigma^2}_y$ is the variance of y;
σ_{xy} is the covariance of x and y
$c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$, two variables to stabilize the division with weak denominator.
L is the dynamic range of the pixel-values.
$k1 = 0.01 \ and \ k2 = 0.03$ by default.

The Normalized correlation coefficient (NCC) is used to measure robustness. It calculates the difference between the original and stego image. It may be defined as:

$$NCC = \frac{\sum_{i=1}^{Row}\sum_{j=1}^{Col} x(i,j)y(i,j)}{\sum_{i=1}^{Row}\sum_{j=1}^{Col} |x(i,j)|^2} \tag{4}$$

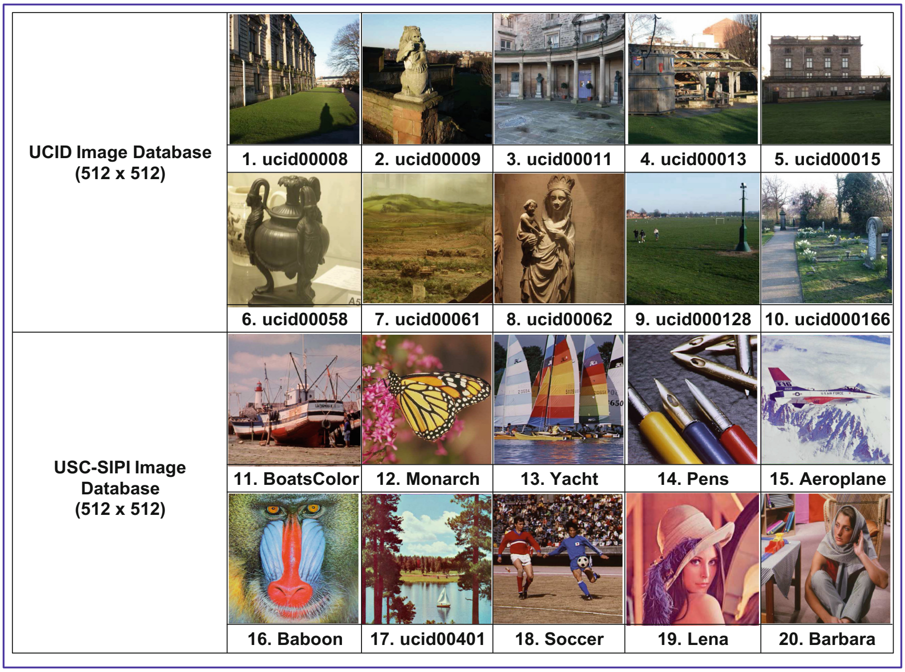

Fig. 3. Stego images with (512 × 512) pixel after embedding data.

where Row and Col are the number of row and column in the images, respectively, x(i, j) and y (i, j) are the original cover image and the stego image respectively. Figure 3 shows the stego images after embedding secret data. Experimental results of our proposed scheme in terms of different comparison metrics are shown in Tables 2, 3, 4 and 5.

Table 2. The comparison table of our proposed scheme with respect to PSNR, SSIM, NCC

Image database	Cover image	PSNR	SSIM	NCC
USC - SIPI image database (512 × 512)	BoatsColor	45.32	0.996	0.996
	Monarch	42.3	0.996	0.996
	Yatch	41.96	0.996	0.996
	Pen	43.25	0.996	0.996
	Aeroplane	44.32	0.996	0.996
	Baboon	45.32	0.996	0.996
	Sailboat	42.3	0.996	0.996
	Soccer	41.96	0.996	0.996
	Lena	43.25	0.996	0.996
	Barbara	44.32	0.996	0.996
UCID image database (512 × 512)	Ucid00008	48.3	0.996	0.996
	Ucid00009	47.6	0.996	0.998
	Ucid00011	45.3	0.996	0.996
	Ucid00013	48.6	0.996	0.946
	Ucid00015	48.3	0.996	0.996
	Ucid00058	47.6	0.996	0.998
	Ucid00061	45.3	0.996	0.996
	Ucid00062	48.6	0.996	0.946
	Ucid00128	48.6	0.996	0.946
	Ucid00166	44.7	0.996	0.996

Table 3. Comparison with other schemes with respect to execution time

Techniques	Execution time for embedding
Singh and Singh [8]	19.7653 s
Kim and Lee [4]	11.82 s
Lutovac [3]	2.36 s
Proposed scheme	2.25 s

Table 4. Comparison table with respect to PSNR, NCC and execution time for embedding

Image	Singh and Singh [8]			Rahman et al. [6]			Proposed scheme		
	PSNR	NCC	Execution time	PSNR	NCC	Execution time	PSNR	NCC	Execution time
Lena	39.7928	0.9973	19.6405	31.4550	0.9976	...	49.92	0.9998	2.2365
Boat	39.9285	0.9984	19.7653	30.0704	0.9980	...	47.25	0.9996	2.1565
Baboon	39.5467	0.9980	19.8433	30.4195	0.9906	...	48.46	0.9989	2.2641
House	39.1570	0.9981	19.9525	31.4114	0.9959	...	48.39	0.9984	2.2741
Pepper	40.1907	0.9980	19.9993	30.5127	0.9945	...	46.92	0.9985	2.2947
Zelda	39.7255	0.9980	19.6405			...	47.89	0.9991	2.1851
Aeroplane	...	...	...	...	...	...	46.33	0.9979	2.1894

Table 5. Comparison scheme with the other scheme in terms of PSNR and payload

Cover image	Lin and Shiu scheme [2]		Saidi scheme [7]		Wei et al.'s scheme [10]		Our proposed scheme	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	90,112	35.28	163,840	36.3762	64,008	33.971	36864	49.92
Airplane	90,112	34.53	163,840	36.7870	64,008	31.949	36864	46.33
Boat	90,112	33.05	163,840	34.4317	64,008	31.147	36864	47.25
Baboon	90,112	28.22	163,840	26.4209	64,008	25.995	36864	48.46
Peppers	90,112	35.09	163,840	35.6165	64,008	33.400	36864	46.92

5 Steganalysis and Evolution

The proposed data scheme is highly robust and only authorized person can extract the secret image by using proper weighted matrix. Six different numbers are required to form the weighted matrix. Also the sequence of numbers in the weighted matrix should be proper. Even if a single number is different in weight matrix or the sequence of these numbers are different, the recovery of the secret image is not possible. This increases the robustness of the proposed scheme.

6 Conclusion

In this paper, a secured stenographic scheme using weighted matrix in discrete cosine transform domain is proposed. Here, to embed confidential messages a shared secret key in the form of a matrix is used. The PSNR is reasonable and higher than 47 dB. In this scheme it is possible to embed more bits per block by applying weight matrix more than once to get higher bits per pixel. But in that case the PSNR will be as low as around 30 dB which makes the image vulnerable for attacking.

For future research, some authentication features can be included into the recent technique. This not only can be used for authentication but also can introduce some randomness and other extra security features into the proposed scheme. Also the idea of using weighted matrix may be used in other transform domain in order to improve results of steganography.

References

1. Chang, C.C., Lin, C.C., Tseng, C.S., Tai, W.L.: Reversible hiding in DCT-based compressed images. Inf. Sci. **177**, 2768–2786 (2007)
2. Lin, C.C., Shiu, P.F.: High capacity data hiding scheme for DCT-based images. J. Inf. Hiding Multimed. Signal Process. **1**(3), 220–240 (2010)
3. Lutovac, B., et al.: An algorithm for robust image watermarking based on the DCT and Zernike moments. Multimed. Tools Appl. **76**(22), 23333–23352 (2017)
4. Kim, H.S., Lee, H.-K.: Invariant image watermark using Zernike moments. IEEE Trans. Circuits Syst. Video Technol. **13**(8), 766–775 (2003)
5. UCID Image Database, Nottingham Trent University, UK. http://jasoncantarella.com/downloads/ucid.v2.tar.gz
6. Rahman, M.M., et al.: A semi blind watermarking technique for copyright protection of image based on DCT and SVD domain. Global J. Res. Eng. (2017)
7. Saidi, M., et al.: A new adaptive image steganography scheme based on DCT and chaotic map. Multimed. Tools Appl. **76**(11), 13493–13510 (2017)
8. Singh, D., Singh, S.K.: DCT based efficient fragile watermarking scheme for image authentication and restoration. Multimed. Tools Appl. **76**(1), 953–977 (2017)
9. University of Southern California: The USC-SIPI Image Database. http://sipi.usc.edu/database/database.php
10. Wei, S., Zhe-Ming, L., Yu-Chun, W., Fa-Xin, Y., Rong-Jun, S.: High performance reversible data hiding for block truncation coding compressed images. Signal Image Video Process. **7**(2), 297–306 (2013)
11. Weng, C.-Y., Huang, C.-T., Kao, H.-W.: DCT-based compressed image with reversibility using modified quantization. In: Pan, J.-S., Tsai, P.-W., Watada, J., Jain, L.C. (eds.) IIH-MSP 2017. SIST, vol. 81, pp. 214–221. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-63856-0_27