IEIT 2022

The 2nd International Conference on Electrical and Information Technology

CERTIFICATE

No: 21115/PL2/DL/2022

this certificate is presented to

Lusia Rakhmawati

for participating as a PRESENTER for the paper entitled

Block-Based Image Reversible Data Hiding Based on the Visual Feature and Edge Entropy

in IEIT 2022

The 2nd International Conference on Electrical and Information Technology

"Science, Technology, Innovative Academic and Vocational Research Towards Product Development Through Industrial and Educational Cooperation"

September 15th-16th, 2022

Director

Supriatna Adhisuwignjo, ST., MT.
NIP. 197101081990031001

Conference Chair

Dr. Eng. Rosa Andrie Asmara, ST., MT.
NIP. 198010102005011001

Block-Based Image Reversible Data Hiding Based on the Visual Feature and Edge Entropy

Lusia Rakhmawati
Department of Electrical Engineering
Surabaya State University
Surabaya, Indonesia
lusiarakhmawati@unesa.ac.id

Hapsari Peni Agustin Tjahyaningtijas
Department of Electrical Engineering
Surabaya State University
Surabaya, Indonesia
hapsaripeni@unesa.ac.id

Wiyli Yustanti
Department of Informatics
Surabaya State University
Surabaya, Indonesia
wiyliyustanti@unesa.ac.id

***Abstract*—Due to the widespread usage of the Internet, electronic information can be quickly altered, duplicated, and shared across interconnection. As a result, the unauthorized reproduction of digital material became a severe issue. Reversible data hiding (RDH) was a practical way of protecting digital media's copyright. This research presents an enhanced DCT-based RDH method that considers human visual features. A less uniform block was used for the information embedding to achieve high imperceptibility for a block based RDH technique. The testing findings of the suggested technique shown a better increase in robustness and non - repudiation under various kinds of image alteration procedures.**

Keywords—Reversible data hiding, block selection, Discrete Cosine Transformation, visual entropy, edge entropy

I. Introduction

The simplicity of creating and distributing digital material has significantly grown because of the enormous rise of online and smart technology in recent years. The issue has made it simpler than ever to use multimedia items illegally and erratically. It becomes critical to safeguarding digital product ownership while enabling full use of Internet resources. One technology strategy to protect intellectual property rights for digital products is data hiding. Reversible data hiding (RDH) [1][2] is a form of data hiding that allows the host sequence and embedded data from the tagged pattern to be restored without resulting in any information leakage. In fields where the original signal is so priceless that it cannot be corrupted, such as medicine, the military, and legal forensics, this crucial approach is frequently applied. By using the reverse procedure and the right keys, it is possible to extract the secret information [3].

Most RDH techniques used in early research are based on lossless compression [4],[5].[6] The general idea is to space out reversible data embedding by lossless compressing some aspects of the original image. These first techniques frequently have a low embedding capacity and may seriously impair image quality. To improve performance in this context, more effective RDH approaches have been suggested, such as difference expansion (DE) [1][7] and histogram shifting (HS) [3][8].

Most RDH methods are designed to work with uncompressed images, and in recent years, Visual quality and embedding capability have seen substantial improvements. They are not always instantly applicable to Joint Photographic Experts Group (JPEG) images[5][2].

RDH in a JPEG image has a variety of applications including archive management [3][5] and image authentication [5]. Even if most users will not notice the distortion, an image source might not want actual content modified in multimedia archives since it would cost too much storage space to keep both the real and the modified copies. A minor change to a picture may not be what the image's creator desires for image authentication. RDH should be the best solution in these cases since it can both detect tampered regions and retrieve the original image content.

Because JPEG is a compressed format, the packet size of the uncompressed deformation approach is severely limited. Additionally, this approach could result in a material increase in file size and poor visual quality. Another approach is based on modified JPEG quantization tables that were initially proposed in [9] and later improved by Wang et al. [1]. The concept is quite straightforward and useful. By dividing some entries of the quantization table by the same integer and multiplying the associated quantized DCT coefficients by the same integer, space for information embedding may be created (additionally adding an adjustment flag if necessary). This approach makes it simple to achieve high quality and a sizable capacity.

In this study, we provide an improved DCT-based RDH approach that uses a block-based RDH method and considers HVS features. To attain high imperceptibility for a block based RDH system, a less uniform block was employed for data embedding. To achieve the appropriate performance level for the recommended RDH technique, an entropy is helpful when it comes to coding images since it sets a lower limit on the average bit length per pixel that can be achieved by the best coding technique without losing any data. The visual feature and edge entropy are two elements that support the selection of the data embedding areas. The DCT is then applied to the selected image blocks. By changing the entries in each selected DCT coefficient with the least degree of distortion, the information is embedded into the selected blocks while maintaining the visual quality of the data-concealed images and boosting its durability. The strategy can meet the RDH system's imperceptibility and resilience requirements.

The substance of this article is formatted as follows. Section 2 presents the proposed RDH strategy. In Section 3, simulations of our approach against attacks are carried out. Finally, Section IV concluded this paper.

2022 International Conference on Electrical and Information Technology (IEIT) | 978-1-6654-5303-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/IEIT56384.2022.9967877

II. The Proposed Method

The suggested data hiding scheme is described in detail in this section. Fig. 1 depicts the embedding processes.

A. Data on images

Two opposing needs must be satisfied when constructing a data concealing method: (1) the hidden message must be undetectable, and (2) the secret message must be robust and challenging to remove. The payload should be included into the host medium's perceptually most important elements to create more reliable RDH techniques [11]. Several well-known research projects use HVS characteristics to build a more reliable payload. In addition to measuring and controlling marked perceptibility after embedding, the HVS model may also be applied while embedding. As a result, we selected the best locations for data embedding based on edge entropy and visual entropy, which are also used by [5].

A important technique for describing an image region is to quantify its texture content. A common statistic for characterizing the texture of a picture is the visual entropy. The standard mathematical formula for calculating visual entropy is shown in Eq. 1. According to Shannon's definition, an n-state system's entropy is

$$H_1 = -\sum_{k=1}^{n} p_k \log p_k \qquad (1)$$

p_k is the probability that the event will happen "k" with $0 \le p_k \le 1$ and $\sum_{k=1}^{n} p_k = 1$. The cooccurrence of the pixel values is not considered; The probability distribution of the pixel intensities is the only factor influencing the result. Therefore, the H_1 is thought of as an image-wide measurement.

The pixel intensities of a picture do, however, have some dependency. To determine the entropy, consider the dimensional relationship between the grayscale elements of certain pixels in an area. The edge of an image can be regarded as a crucial component of the picture since it can be identified by comparing the pixel values for local characteristics recorded in pairs of non-overlapping areas bordering the pixel. As a result, in addition to visual entropy, edge entropy of an image block is taken into account while picking embedding regions. Eq. 2 gives the definition of edge entropy.

$$H_2 = \sum_{k=1}^{n} p_k exp^{1-p_k} \qquad (2)$$

The key measures taken to combine block selection for data embedding with the HVS model are as follows: (1) In the first stage, a cover picture is separated into n non-overlapping blocks. Each block's edge and visual entropies are determined using equations (1) and (2), respectively. (2) Each block's two entropy measurements are then added up, and the values that result are arranged in ascending order according to their magnitude. The block with the lowest value is picked to insert the data until the number of selected blocks equals the size of the payload.

B. The embedding procedure

An adjustable scale factor was used to construct the process for embedding resilient RDH systems utilizing DCT. Fig. 1 depicts the block diagram of the embedding system used in this investigation.

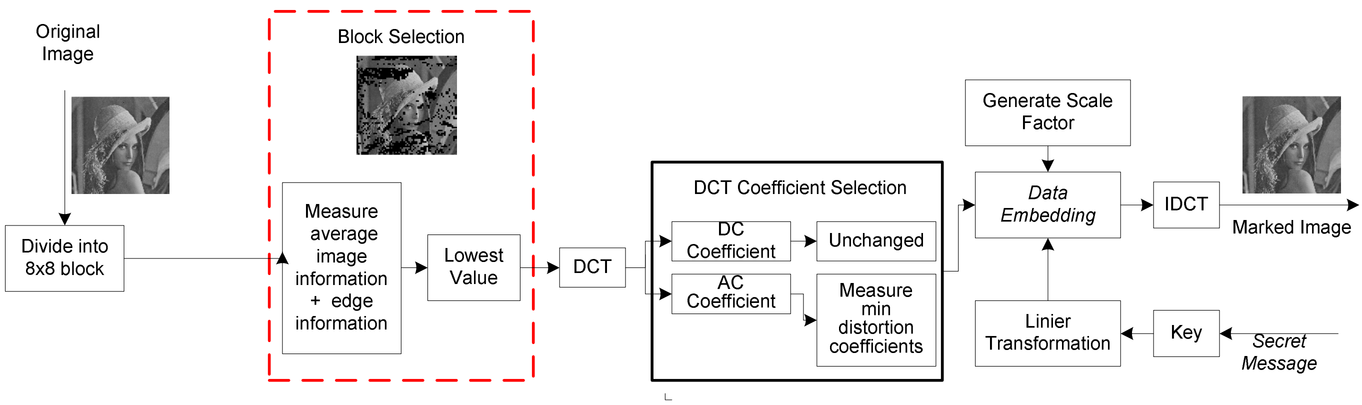


Fig. 1. The Proposed Embedding Procedure

Step 1: The cover picture is initially segmented into 8 x 8-pixel non-overlapping parts.

Step 2: Using the HVS characteristics as Eq. 1 and Eq. 2, choose the relevant blocks for embedding the data payload.

Step 3: To generate the DCT domain frequency bands, implement the DCT process to the selected blocks.

Step 4: Apply coefficient selection by considering the quantized DCT coefficient values' distribution properties, specifically by choosing the component with the least distortion as used by [12].

Assuming that a block's embedding capacity is T_k and its shifting capacity is U_k, the technique for choosing the insertion point in each block is then established. If a coefficient selection technique has a large insertion capacity but a modest displacement capacity, it is said to be successful. The insertion capacity may be estimated by counting the coefficients "1" and "-1" in each, whereas the total displacement capacity can be computed by adding together all the coefficients that are not zero. is the outcome of each k-DCT block's transformation, and B is the quantizer's output, which is the quantized DCT coefficient on the k-block.

For the embedding of a secret message that considers the number of sub-channels, the effective frequency selection, F, where each pixel has the coordinates of the quantized AC coefficient that is the position of the sub-channel s, $s \in 1, 2, 3, \ldots 63$. The AC coefficient of embedding and shift capacity that produces the minimum distortion value is calculated through the effective frequency using Eq.3

$$F = \sum_{k=1}^{\frac{MxM}{64}} \frac{\left(\left(\frac{1}{2}T_k + U_k\right) \times MSE(B_k - A_k)\right)}{T_k} \quad (3)$$

Step 5: Generate Scale factor to represents the location of the best coefficients because of the experiment at intermediate frequencies. The scale factor is more than zero which used in [13].

Step 6: Data embedding is done by first randomizing the position of the secret message using a linear transformation. Before further processing, block mapping is performed A→B→C→D→⋯→A to encrypt secret data information. The feature intensity of block A will be attached to block B and Using the 1-D transformation technique developed in [7], the feature intensity of block B will be connected to block C, and so on to produce a one-to-one mapping series in this study using Eq. 4. The steps to get a random block mapping are as follows and the pseudo code for this mapping can be seen in algorithm 1.

$$B' = [f(B) = (K \times B) mod\ N] + 1 \quad (4)$$

Notation B, B' [1, N], K represents a private key, and N represents the total number of blocks in the image.

Algorithm 1. Random Block Mapping

INPUT: Block row B_b with index number b, $1 \leq b \leq N$, K_1

Procedure Mapping series generation

$B'_c \leftarrow [f(B_b) = (K_1 \times b) mod\ N] + 1$ ⊳ K_1 is a primary number

End

OUTPUT: Mapping block array B'_c with index number c

Step 7: Apply inverse DCT procedures to each of the chosen blocks will produce the marked image.

C. The extraction procedure

The following steps make up the data hiding extraction sequence:

Step 1: 8 × 8-pixel non-overlapping blocks are first created from the marked image.

Step 2: To identify the block in which the data is embedded, each block's visual and edge entropies are calculated.

Step 3: To obtain DCT domain frequency bands, apply DCT to the chosen blocks.

Step 4: The data payload is removed. A positive difference denotes the extraction of a bit 1, whereas a negative difference suggests the extraction of a bit 0. The recovered bit values are then used to produce the extracted bit.

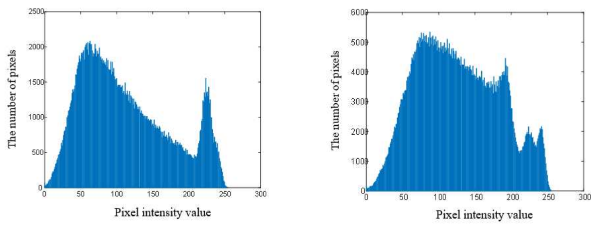
III. Experimental Results

Fig. 2 illustrates how the secret message bits are generated at random in all our experiments using the test images Lena, Lake, and Baboon. The average amount of message bits that may be placed in images. The suggested method's visual quality and file size were compared to three state-of-the-art techniques [3, 14] to determine its effectiveness. The visual quality of the marked JPEG image is evaluated using the PSNR, which is calculated between the marked JPEG image and the original JPEG image. A file's size is calculated in terms of bytes. Take note that QF=50 was used for all trials.

Fig. 3 displays an example of the outcomes of data embedding for Baboon image. Since the human eye perceives these findings as having the same appearance, histogram results are added for each image to help explain the variations. In this case, the marked picture of the initial Baboon image and the consequences of the input images are differentiated from one another.

(a) (b) (c)

Fig. 2. Test Images: a. Lena. b. F16 Airplane. c. Baboon



(a) (b)

Fig. 3. Baboon image histogram. (a) Original image. (b) Marked Image

A. Marked Image Quality

The PSNR is created in order to measure the visual quality of the original and annotated JPEG images. To address the visual appeal of the cover picture and preserve the key statistical characteristics of the image after embedding, researchers developed a distortion function [3]. It is shown in Table I. However, as the payload increases, it eventually converges to [14], despite the experiment showing that the suggested technique has the highest PSNR of all the preceding research. This is because choosing the location of the AC coefficient has no effect when employing all of the AC coefficients for embedding.

The PSNR values for the three photos described in Table I are presented numerically. The recommended method performs the best based on the tables. Given that the AC coefficient selection approach involves only a tiny amount of additional calculation when compared to [14], the proposed method's results seem to be highly impressive.

B. File Size Preservation

It is obvious that while hiding JPEG data, the file size must be considered along with image quality. The proposed method typically results in a marked image with smaller file size than the methods that came before it (Table II). The tables show that the proposed method generally results in the shortest file size, but [14] appears to do so for some images. Bytes are used to determine a fisle's size. Due to the proposed method's use of the same HS-based embedding technique as the Huang et al method the discarded test images for the two approaches will be equivalent. The advantages of our bitstream expansion become more obvious at QF = 100, and the suggested technique consistently produces smaller enhanced file sizes than those of the Huang et al method. We have two main advantages: first, host quantified DCT coefficients are selected for embedding while taking frequencies into account; second, an improved block selection approach is employed.

TABLE I. COMPARISON OF PSNR (dB) WITH AN 8000 AND 16000 BITS PAYLOAD

Image	8000 bits			16000 bits		
	***Method* [14]**	*Method* [3]	***Pro-posed***	***Method* [14]**	*Method* [3]	***Proposed***
Lena	45.24	45.53	46.3	39.71	40.13	40.84
F16	44.24	45.03	45.8	38.26	39.15	39.87
Baboon	42.49	42.83	43.77	36.95	37.92	38.54

TABLE II. AN INCREASE IN FILE SIZE (IN BYTES) WITH 8000 BITS AND 16000 BITS PAYLOAD

Image	8000 bits			16000 bits		
	***Method* [14]**	***Method* [3]**	***Pro-posed***	***Method* [14]**	*Method* [3]	***Proposed***
Lena	1305	1174	1222	2261	2149	2128
F16	1169	1130	1125	2220	2141	2136
Baboon	1286	1188	1546	2633	2575	2493

IV. CONCLUSION

This study offers a JPEG image reversible data hiding technique based on AC coefficient DCT and human visual characteristics. Prior to embedding, block order is carried out, and sections that are suitable for embedding are selected based on the distortion sum of the AC coefficients in a section to have the best coefficients for RDH. HVS features may be used to choose hidden information embedding zones that strike a good compromise between the resilience and quality of the tagged picture. The proposed technique has demonstrated imperceptibility in experimental outcomes. Future research will make use of additional perceptual features and more sophisticated perceptual models.

ACKNOWLEDGMENT

This Publication is enabled through National Competitive Base Research Grant No. 126/E5/PG.02.00.PT/2022 from Directorate General of Higher Education, Research, and Technology, The Ministry of Education and Culture of The Republic of Indonesia.

REFERENCES

[1] W. Wang, J. Ye, T. Wang, and W. Wang, "Reversible data hiding scheme based on significant-bit-difference expansion," 2017.

[2] H. Sakai, M. Kuribayashi, and M. Morii, "Adaptive reversible data hiding for JPEG images," *2008 Int. Symp. Inf. Theory its Appl. ISITA2008*, pp. 7–10, 2008.

[3] F. T. Wedaj, S. Kim, H. J. Kim, and F. Huang, "Improved reversible data hiding in JPEG images based on new coefficient selection strategy," *Eurasip J. Image Video Process.*, vol. 2017, no. 1, pp. 1–11, 2017.

[4] Y. S. Chen and R. Z. Wang, "Reversible authentication and cross-recovery of images using (t, n)-threshold and modified-RCM watermarking," *Opt. Commun.*, vol. 284, no. 12, pp. 2711–2719, 2011.

[5] S. Kim, F. Huang, and H. J. Kim, "Reversible data hiding in JPEG images using quantized DC," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 9, pp. 1610–1621, 2016.

[6] R. Chamlawi and A. Khan, "Digital image authentication and recovery: Employing integer transform based information embedding and extraction," *Inf. Sci. (Ny).*, vol. 180, no. 24, pp. 4909–4928, 2010.

[7] J. Zhou and O. C. Au, "Determining the capacity parameters in PEE-Based reversible image watermarking," *IEEE Signal Process. Lett.*, vol. 19, no. 5, pp. 287–290, 2012.

[8] K. Wang, G. Chen, Q. Ai, H. Cao, P. Zhou, and D. Wu, "Reversible data hiding based on structural similarity block selection," *IEEE Access*, vol. 8, pp. 20375–20385, 2020.

[9] M. El'arbi and C. Ben Amar, "Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain," *IET Image Process.*, vol. 8, no. 11, pp. 619–626, 2014.

[10] S. Roy and A. K. Pal, "An indirect watermark hiding in discrete cosine transform–singular value decomposition domain for copyright protection," *R. Soc. Open Sci.*, vol. 4, no. 6, 2017.

[11] D. Hou, H. Wang, W. Zhang, and N. Yu, "Reversible data hiding in JPEG image based on DCT frequency and block selection," *Signal Processing*, vol. 148, pp. 41–47, 2018.

[12] L. Rakhmawati, W. Wirawan, S. Suwadi, C. Delpha, and P. Duhamel, "Blind robust image watermarking based on adaptive embedding strength and distribution of quantified coefficients," *Expert Syst. Appl.*, vol. 187, no. September 2021, p. 115906, 2022.

[13] L. Rakhmawati, "Blind Robust and Self-Embedding Fragile Image Watermarking for Image Authentication and Copyright Protection with Recovery Capability," vol. 13, no. 5, 2020.

[14] F. Huang, X. Qu, H.J. Kim, Reversible data hiding in JPEG image. IEEE Trans. Circuits Syst. Video Technol. 26(9), 1610–1621 (2016)