IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 41, No. 3, June, 2024, pp. 1507-1515
Journal homepage: http://iieta.org/journals/ts

Digital Documents Integrity Protection Using Invisible Changeable Watermark

Ahmad M. Nagm[1], Mohamed Shehata[1], Ahmed S. Salama[1,2], Mohamed S. Abdallah[3,4,5], Young-Im Cho[5]*, Mohammed Elwan[6]

[1] Department of Computer Engineering and Electronics, Cairo Higher Institute for Engineering, Computer Science and Management, Cairo 11477, Egypt
[2] Department of Electrical Engineering, Faculty of Engineering & Technology, Future University, New Cairo 11835, Egypt
[3] Informatics Department, Electronics Research Institute (ERI), Cairo 11843, Egypt
[4] AI Laboratory, DeltaX Co., Ltd., Seoul 08213, Republic of Korea
[5] Department of Computer Engineering, Gachon University, Seongnam 13415, Republic of Korea
[6] College of Computing and Information Technology, Arab Academy for Science, Technology and Maritime Transport (AASTMT), Smart Village, B 2401, Giza 12577, Egypt

Corresponding Author Email: yicho@gachon.ac.kr

https://doi.org/10.18280/ts.410338

Received: 9 November 2023
Revised: 28 February 2024
Accepted: 29 March 2024
Available online: 26 June 2024

Keywords:
integrity protection, image, watermark, hiding capacity of images, optical character recognition

ABSTRACT

One of the strategies used to secure the integrity of digital documents is invisible watermarking. In this research, a secure invisible image watermarking technique is developed to identify any changes or tampering within the document's content. The suggested watermark has the benefit of being based on the document's content rather than putting one image into another. The proposed watermark is changeable and determined by the word order of the text and the number of letters in each word. The proposed approach is divided into three steps. In the beginning, the document's image is converted into text using Optical Character Recognition (OCR). The second step is the mapping of the letters of the text using the American Standard Code for Information Interchange (ASCI) II. Finally, the watermark bit is hidden using a recommended watermark embedding procedure in each pixel's least significant bit (LSB). The main target of the traditional algorithms is how to extract the watermarked image from the original one. The proposed watermark identifies the position of any deliberations and preserves the watermark and the information at the same time. A JPG image is used to evaluate the suggested algorithm and the findings demonstrate that the proposed algorithm has a strong capacity to retain the content of the document and to identify any modifications. The code takes 1.5 seconds to test if the document has been tampered with. The Structural Similarity Index (SSIM) is 0.99998, the Peak Signal Noise Ratio (PSNR) is 69.149, the Mean Absolute Error (MAE) is 0.0028, the Universal Image Quality Index (UIQI) is 0.99998, and the Mean Square Error (MSE) is 0.00791.

1. INTRODUCTION

Digital storage, signal processing, and communication infrastructure developments in recent years have made it possible to distribute digital media widely. Multimedia commerce transactions benefit from the introduction of a flexible and affordable business strategy brought about by digital distribution. The fact that the information is digital also makes it possible for anybody to edit, copy, or access material outside of the restrictions specified for the specific transaction. In regard to this, integrity protection has gained significance in the field of digital technology. It's critical to be able to check the model's integrity once it's been deployed into a safety-critical system to ensure that it hasn't been tampered with.

The performance impact has been neglected in most relevant studies on cryptography and copyright protection for authentication and integrity protection due to their high complexity and relatively considerable redundant implementation overheads. This is particularly true for more straightforward applications where integrity protection and authentication confirmation are the only requirements.

There are other explanations for why encryption by itself isn't always a perfect answer in some situations. For example, sending data without any secrecy or unnecessary expense may be better in certain applications, where encryption involves resource overheads. Other situations include those in which some network management protocols distinguish between integrity and confidentiality, making encryption on its own unacceptable.

A watermarking approach is used to embed a watermark into the model to be protected and verify the system's integrity by checking if the watermark is intact to achieve this goal.

Digital watermarking is an area of computer security that deals with the protection of digital things in a broad sense. Watermarking differs from digital signatures in that a watermark signal is embedded directly into the digital host object. This distinguishes watermarking from digital signatures, a set message embedded in digital files. This hidden information is later utilized to determine who owns the data.

Many watermarking algorithms have been designed with various goals in mind, but they all have the same high-level structure; in general, watermarking an object includes two complementary actions [1].

The first one is embedding, which is done just once and, in most cases, off-line, thus it may take up more computing resources than the second operation. The embedding step embeds a watermark sequence into the host object. A secret key to make the entire process safe, or to improve its security. The validation is the second step: this method is carried out every time they need to check if an object has a watermark signal arise, thus a light and quick approach is recommended.

The specific requirements of each watermarking application dictate the features that must be included in the system and influence the methods chosen for embedding and detecting the watermark. Real-world system characteristics that are often discussed include the data capacity of the watermark, visibility of the embedded mark, immunity of the detector to false alarms, security, and various forms of robustness against distortion (caused by routine processing operations or changes in geometry) and attack [2, 3]. One feature that isn't as frequently discussed but is crucial for numerous real-world applications is performance, or the speed at which the watermark is detected and embedded.

The main objective of this research paper is to secure the transfer of digital documents. The following is the contribution of this study:

- The proposed code detects forgery in the text without the need to compare it with the original text and also locate the forgery.
- Its benefit over other methods is that the generated code is spread across the whole test image, not only in the non-interest pixels.
- The proposed algorithm detects the location and the number of tampered words.
- The watermark is dynamic and based on word information, it protects the watermarked item from both unintentional and intentional attacks, and the watermark signal cannot be retrieved by unauthorized entities.
- The weight values are modified in the least significant bits (LSB), the distortion caused by the watermark embedding is lower than that introduced by the method for images.
- Light and fast integrity check: Since each word has its watermark, it is easy to discover any tampering.
- It overcomes the difficulty that occurs in spatial domain algorithms that cannot provide both robustness and protection against intentional attacks.

The study paper is structured as follows: in Section 2, the most recent studies in this topic were examined, along with the most recent research findings. The suggested approach design is shown in Section 3. In Section 4, the findings are examined, and the effectiveness of the suggested algorithm is ascertained. Lastly, Section 5 is conclusion.

2. RELATED WORKS

Day by day the amount of information and data transferred on the Internet is increasing, especially on social community platforms. Moreover, with the rapid advancement of image processing tools, it has become easier to change data and images as they are being transferred. Transferring exams via the Internet and securing them against deliberate change has become one of the most important problems facing workers in the educational aspect.

In addition to standard cryptographic techniques [4-7], watermarking has been proposed to solve the above concern [8-29]. Watermarking is a technique for achieving image authentication and tamper detection by embedding watermark bits into the original image [25].

The watermarking idea may be common, but there are different methods to perform it. In recent years, researchers have proposed several watermarking approaches in the spatial domain or frequency domain and recently the Neural Networks.

An invisible watermark is inserted in the cover text to make the trace imperceptible to the readers. In addition, all of the terms in the original text are marked using an instance-based learning method [30].

A wavelet-based copyright certification method was proposed that does not require the original image for watermark verification and uses cryptography technologies like digital signatures and timestamps to make the copyright certification publicly verifiable [31].

An adaptive copyright protection strategy is proposed. This innovative technique allows the owner layer to change the watermark's intensity using a threshold, which can improve the watermarking algorithm's robustness [32].

To counteract model stealing attempts, Szyller et al. [33] altered the neural network's categorization output. Al-onazi et al. [1] proposes a white box watermarking approach for (Deep) Neural Network integrity protection. Because it inserts a watermark bit string into the network's parameters, it may be used with any type of neural network design (deep or shallow).

To summarize the conclusions from previous research:

The splitting of the original image into the region of interest and the region of non-interest is a method used by most known algorithms. The ability of the algorithms to retrieve the watermark from the watermarked image determines their efficiency. The general idea of all watermark algorithms depends on inserting an external image inside the original image as a watermark. Although some of the works relied on watermark verification not to refer to the original image [31], they use the same general idea by inserting an image or logo inside the original image, other than the idea on which the proposed work was based.

This means that the watermark will be included in the region of non-interest, otherwise the image quality will deteriorate. To prove the inaccuracy of the perception. In this work is linked with the watermark while maintaining the image quality. In addition to many tests that the image is subjected to ensure its authenticity, unlike the proposed model.

One of the most important features of the proposed watermark is that it is smart and strict so that the watermark is created for each word within an image and not depending on the image as a whole. The watermark for each word contains the location of the word and the number of its letters, and the letters are converted to binary code using ASCII.

3. SDWM ALGORITHM

The encoder and the decoder are the two main components of digital watermarking systems [34]. To create a watermarked image from a digital document, you'll need an image, a watermark that contains the watermarking information, a security key, and an encoding method to make a watermarked image from a digital document.

Most of the works in the field of watermark depend on separating the image into a region of interest and a region of noninterest and the watermark is created in a region of noninterest.

The suggested watermark is unique in its creation in that it is spread throughout the image words and at the same time, it does not affect the efficiency of the image. The proposed algorithm does not require the original image for watermark verification. For each word in the exam, its watermark is created depending on the word's location and the number of its letters. In the case of forgery, the forged words can be extracted from the watermark. Figure 1 shows the whole proposed watermark procedure.

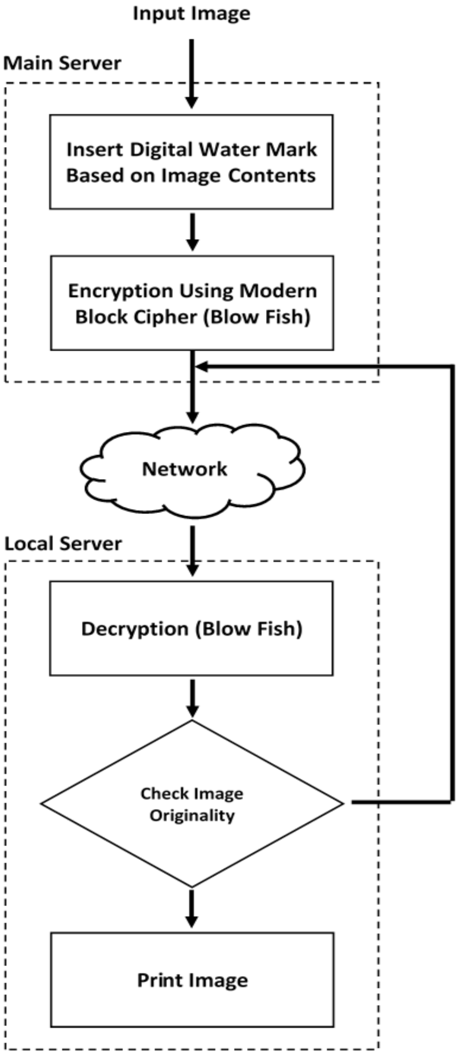

Input Image
Main Server
Insert Digital Water Mark Based on Image Contents
Encryption Using Modern Block Cipher (Blow Fish)
Network
Local Server
Decryption (Blow Fish)
Check Image Originality
Print Image

Figure 1. The whole proposed watermark procedure

The whole structure of the proposed algorithm in the transmitting path is summarized below. Figure 2 illustrates the proposed algorithm in the transmitting path.

- Step1. Read the input image that contains text.
- Step2. Read the image contents (Words) by OCR MATLAB Function.
- Step3. Save the value and locations of the word in the image.
- Step4. Save the boundary boxes for each word.
- Step5. Segment the image into sub-images based on the words.
- Step6. Separate one layer of the image.
- Step7. Create the watermark, merge the word locations, and word characters then convert the merged words to the binary form.
- Step8. Embed the watermark into the isolated layer.
- Step9. Replace the Separated layer with the watermarked layer.
- Step10. Sending the integrity-protected image via an insecure channel.

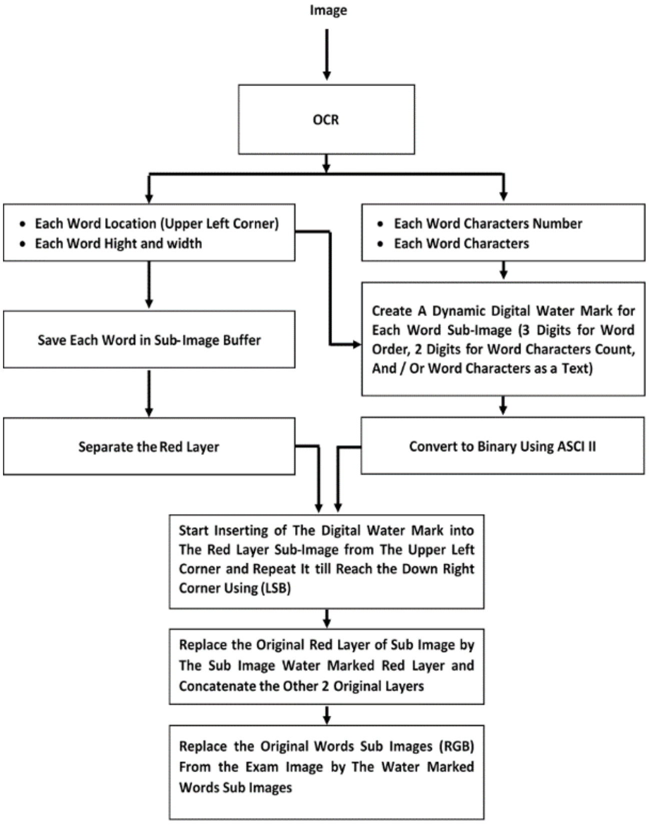


Image
OCR
• Each Word Location (Upper Left Corner)
• Each Word Hight and width
• Each Word Characters Number
• Each Word Characters
Save Each Word in Sub-Image Buffer
Create A Dynamic Digital Water Mark for Each Word Sub-Image (3 Digits for Word Order, 2 Digits for Word Characters Count, And / Or Word Characters as a Text)
Separate the Red Layer
Convert to Binary Using ASCI II
Start Inserting of The Digital Water Mark into The Red Layer Sub-Image from The Upper Left Corner and Repeat It till Reach the Down Right Corner Using (LSB)
Replace the Original Red Layer of Sub Image by The Sub Image Water Marked Red Layer and Concatenate the Other 2 Original Layers
Replace the Original Words Sub Images (RGB) From the Exam Image by The Water Marked Words Sub Images

Figure 2. The proposed algorithm in the transmitting path

The whole structure of the proposed algorithm in the receiving path is summarized below. Figure 3 illustrates the proposed algorithm in the receiving path.

- Step1. Read the integrity-protected watermarked image.
- Step2. Verify the integrity-protected watermarked image.
- Step3. Calculate the words numbers, calculate the boundary boxes, and calculate each word characters.
- Step4. Segment the image into sub-images based on the words.
- Step5. Separate one layer of the image.
- Step6. Calculate the watermark, merge the word locations, and word characters then convert the merged words to the binary form.
- Step7. Extract the embedded watermark.
- Step8. Compare the calculated watermark with the extracted one. If the two watermarks are the same then the image is not tempered, then the image will be printed.

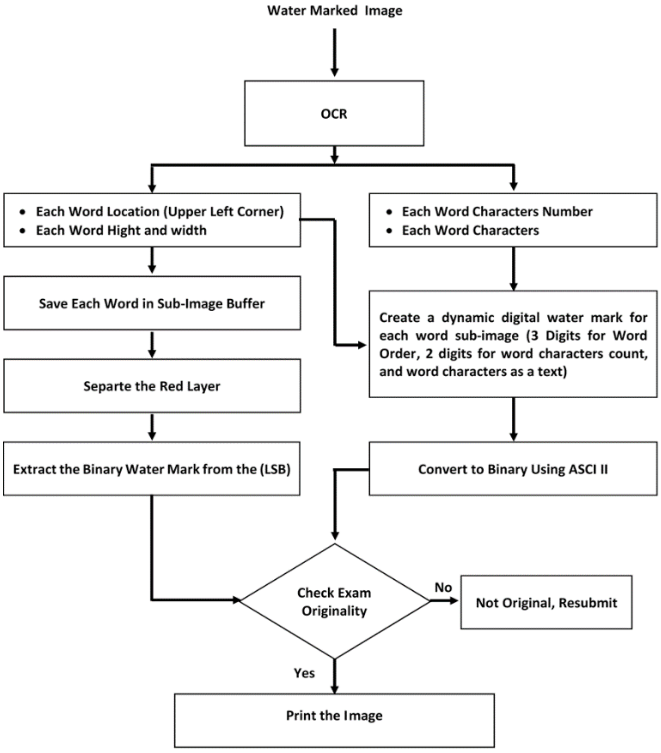

Water Marked Image
OCR
Each Word Location (Upper Left Corner)
Each Word Hight and width
Each Word Characters Number
Each Word Characters
Save Each Word in Sub-Image Buffer
Create a dynamic digital water mark for each word sub-image (3 Digits for Word Order, 2 digits for word characters count, and word characters as a text)
Separte the Red Layer
Extract the Binary Water Mark from the (LSB)
Convert to Binary Using ASCI II
Check Exam Originality
No
Not Original, Resubmit
Yes
Print the Image

Figure 3. The proposed algorithm in the receiving path

Otherwise, the image tempered, and, in this case, the receiver sends a notification to the sender.

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

Through the use of a technique called digital watermarking, identifying information can be subtly and imperceptibly encoded into a data carrier without affecting data usage. This technology frequently safeguards text files, databases, and multimedia content from infringement. The evaluation approach won't be the typical one because the process of creating the watermark is entirely different from that of ordinary watermarks.

There are two categories of attacks on conventional watermarks [31]. The Median Filter attack, JPEG attack, and the Gaussian Noise Attack are examples of conventional attacks. The translation, cropping, rotation, and scaling attacks are some of the Geometrical Attacks.

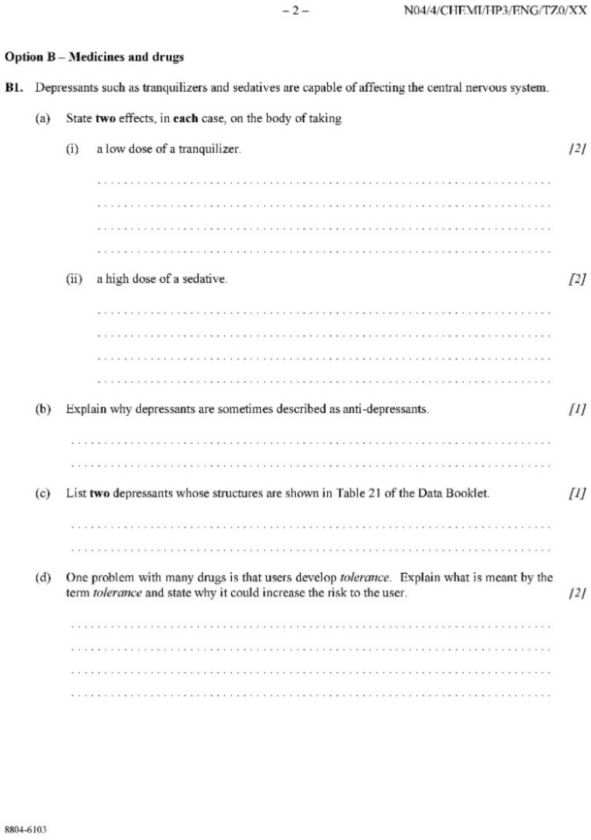
The extraction of the watermarked image from the source image is the primary goal of classical algorithms. However, the goal of the suggested approach is to simultaneously maintain the information and the watermark.

The test platform for the experiment is a 2.3 GHz Intel Core i3 processor with 4GB RAM, using MATLAB 2015 Version 8.5.0.197613.

To illustrate the efficiency of the proposed watermark, it practically applied to one of the International Baccalaureate exams. Figure 4 shows an example of the International Baccalaureate exams.

After reading the exam image, the exam image is converted to text using OCR. The word orders are calculated, and the boundary boxes are detected. Figure 5 shows the detected boundaries.

Each word will be saved in a sub-image. The dynamic digital watermark is created for each word (3 digits for word order, 2 digits for word character count, and 7 bits for each character). The characters are converted to binary using ASCI II.



– 2 – N04/4/CHEMI/HP3/ENG/TZ0/XX

Option B – Medicines and drugs

B1. Depressants such as tranquilizers and sedatives are capable of affecting the central nervous system.

(a) State **two** effects, in **each** case, on the body of taking

(i) a low dose of a tranquilizer. *[2]*

(ii) a high dose of a sedative. *[2]*

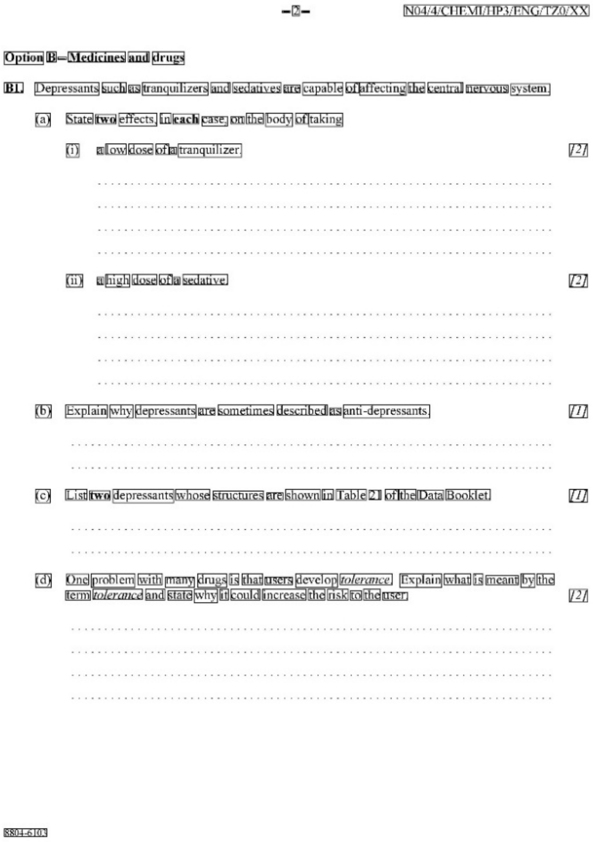
(b) Explain why depressants are sometimes described as anti-depressants. *[1]*

(c) List **two** depressants whose structures are shown in Table 21 of the Data Booklet. *[1]*

(d) One problem with many drugs is that users develop *tolerance*. Explain what is meant by the term *tolerance* and state why it could increase the risk to the user. *[2]*

8804-6103

Figure 4. Sample of the international baccalaureate exam



–2– N04/4/CHEMI/HP3/ENG/TZ0/XX

Option B – Medicines and drugs

B1. Depressants such as tranquilizers and sedatives are capable of affecting the central nervous system.

(a) State **two** effects, in **each** case, on the body of taking

(i) a low dose of a tranquilizer. *[2]*

(ii) a high dose of a sedative. *[2]*

(b) Explain why depressants are sometimes described as anti-depressants. *[1]*

(c) List **two** depressants whose structures are shown in Table 21 of the Data Booklet. *[1]*

(d) One problem with many drugs is that users develop *tolerance*. Explain what is meant by the term *tolerance* and state why it could increase the risk to the user. *[2]*

8804-6103

Figure 5. The detected boundaries

Table 1. ASCII code for the user numbers and letters in the illustrated example

DEC	BIN	Description
48	00110000	Zero
49	00110001	One
50	00110010	Two
51	00110011	Three
54	00110110	Six
97	01100001	Lowercase a
100	01100100	Lowercase d
110	01101110	Lowercase n
111	01101111	Lowercase o
114	01110010	Lowercase r

The following example is to illustrate the idea and learn how to detect manipulation. In Figure 5, which represents a sample of the International Baccalaureate exam, in the first line, we find the word “and”. The word “and” is the number 16 in the text and its number of letters is three letters. According to the ASCII Code in Table 1, the calculated SDWM for ‘and’ is:

1100001100011101101100001100111100001110111011001
00

If we assume that the word “and” is replaced by the word “or” from the same text, we find that the watermark will be changed because the number of letters of the word has changed (two letters), as well as the ASCI code for the word or, and the new watermark will be:

11000011000111011011000011001111011111110010

In the case of replacing the word “and” with the word “or” from outside the text, we find that the watermark is either not present or the watermark is incorrect:

(110001010100101010111100100101010101010).

In all these cases, manipulation will be detected because one of the basics of the code is that the word information is retrieved from the created watermark.

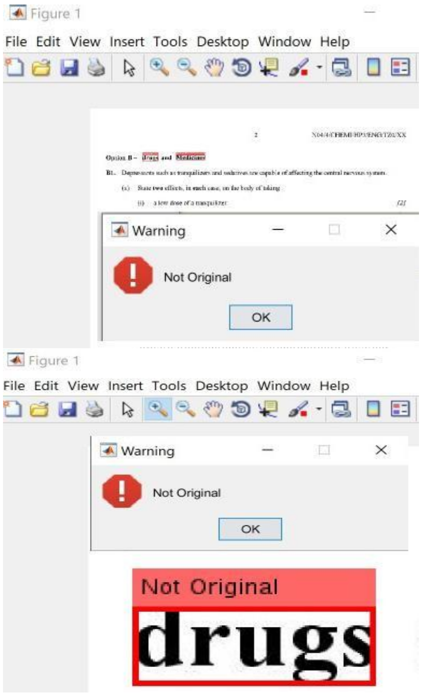


Figure 1
File Edit View Insert Tools Desktop Window Help

2 N04/4/CHEMI/HP3/ENG/TZ0/XX

Option B – drugs and Medicines

B1. Depressants such as tranquilizers and sedatives are capable of affecting the central nervous system.

(a) State two effects, in each case, on the body of taking

(i) a low dose of a tranquilizer [2]

Warning

Not Original

OK

Figure 1
File Edit View Insert Tools Desktop Window Help

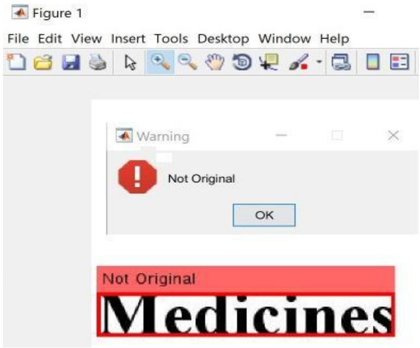
Warning

Not Original

OK

Not Original

drugs



Warning

Not Original

OK

Not Original

Medicines

Figure 6. Detect the location of the tampered words

The position and quantity of tampered words are detected by the suggested algorithm. The capacity of the suggested method to identify the change of two words in the original exam is shown in Figure 6. The word "medicines" was used in place of "drugs" in the example from the previous exam.

Contrary to typical integrity protection, there is a high correlation between neighbouring pixels even though the watermark is included in each word pixel of the text pictures. The comparable correlation between the original and watermarked photographs is displayed in Figures 7 and 8, respectively.

An additional effective feature of the suggested method is the histogram of the original and watermarked image. The histograms of the original and watermarked photographs are shown in Figures 9 and 10.

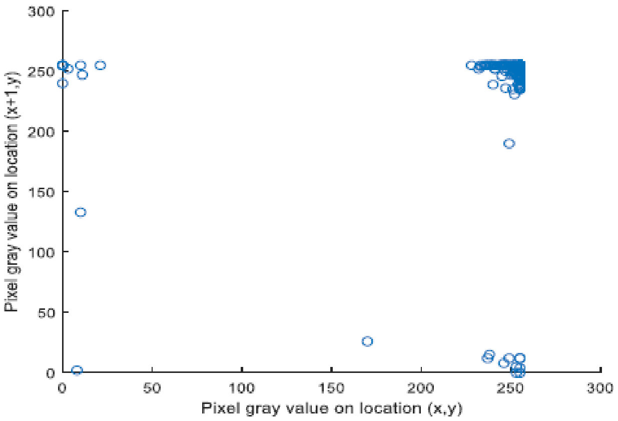


Figure 7. Correlation of adjacent pixels in the original image

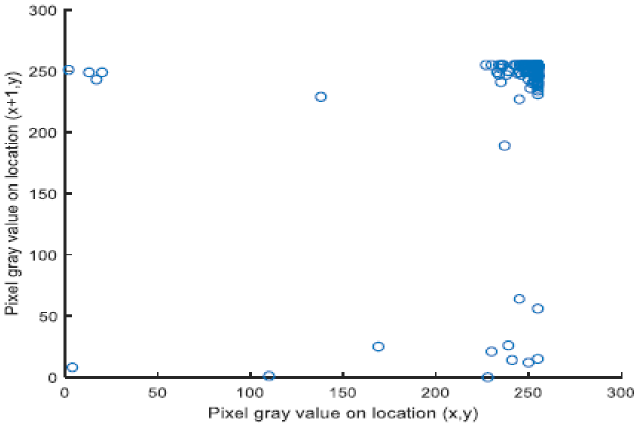


Figure 8. Correlation of adjacent pixels in the watermarked image

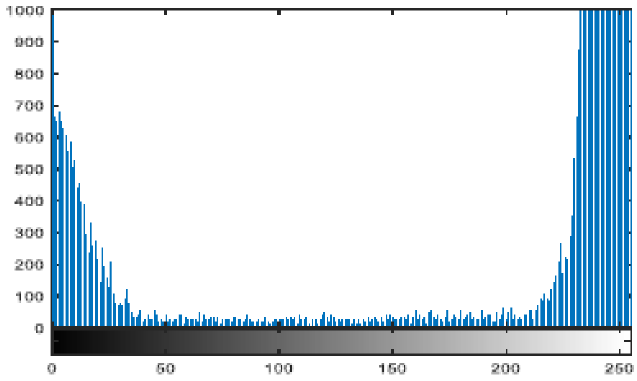


Figure 9. Histogram of the original image

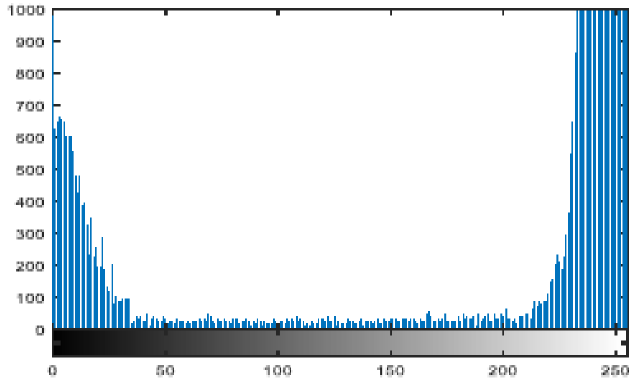


Figure 10. Histogram of the watermarked image

An additional effective feature of the suggested method is the histogram of the original and watermarked image. The histograms of the original and watermarked photographs are shown in Figures 9 and 10.

Our method performs much better than the current state of the art in terms of image evaluation metrics such as PSNR (peak-signal-to-noise-ratio), SSIM (structural similarity index map), UIQI (Universal Image Quality Index), and SSIM [35].

To determine the degree of difference between the original image and the one produced by our proposed model (watermarked image), we employ the following established metrics: MSE, MAE, PSNR, SSIM, and UIQI. A greater PSNR ratio indicates better image creation. The value of SSIM increases as image distortion decreases.

Image distortion: To help with the distortion, the following metrics are used: MSE, MAE, Universal Image Quality Index (UIQI), and Structural Similarity Index (SSIM). The mean squared error (MSE) is computed by averaging the squared intensity differences between the reference image and the watermarked image. The (SSIM) is computed by normalising the mean structural similarity value between the original and watermarked images [34-39]. Any image distortion is modelled by the UIQI.

$$MAE = \frac{1}{N}\sum_{i=1}^{N} \square \, |x_i - v_i| \tag{1}$$

$$MSE = \frac{1}{M * N}\sum_{i=1}^{n} [x(i,j) - v(i,j)^2 \tag{2}$$

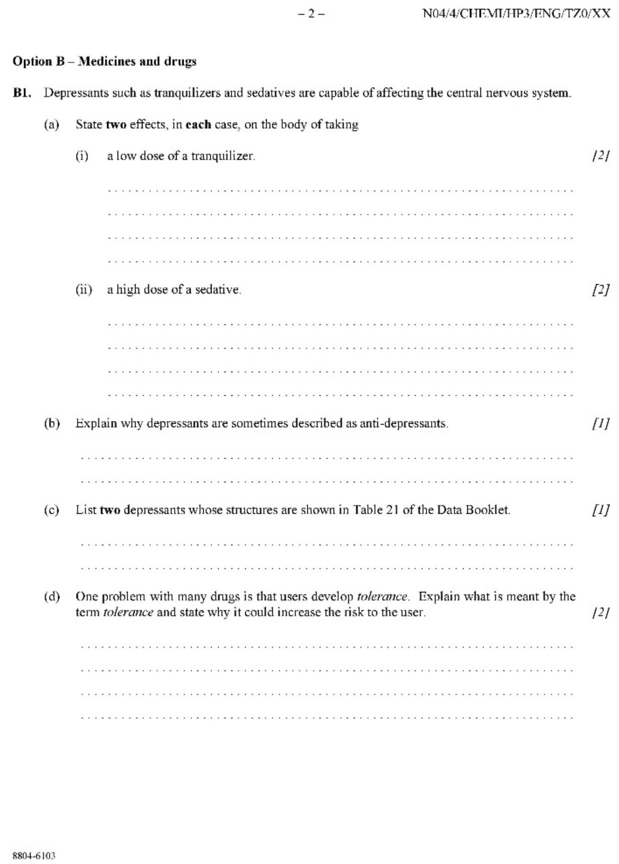
$$\begin{aligned} &SSIM(X,V) \\ &= \left(2 * \underline{x} \, * \underline{v} + c1\right) \\ &* \frac{(2 * \sigma_{xv} + c2)}{\left(\underline{x}^2 + \underline{v}^2 + c1\right) * (\sigma_x{}^2 + \sigma_v{}^2 + c2)} \end{aligned} \tag{3}$$

$$Q = \left(\frac{\sigma_{xv}}{\sigma_x \sigma_v}\right) * \left(\frac{2 * x^{-} * v^{-}}{x^{-2} + v^{-2}}\right) * \left(\frac{2 * \sigma_x * \sigma_v}{\sigma_x{}^2 + \sigma_v{}^2}\right) \tag{4}$$

Imperceptibility: It suggests that the watermarked image and the host image are similar [40, 41].

Invisibility evaluation: The visual quality is measured by contrasting the original and watermarked images' PSNRs [42-44]. Figure 11 makes it evident that there is no discernible difference between the exam with the watermark and the original exam.

$$PSNR = 10(\frac{S^2}{MSE}) \tag{5}$$



– 2 – N04/4/CHEMI/HP3/ENG/TZ0/XX

Option B – Medicines and drugs

B1. Depressants such as tranquilizers and sedatives are capable of affecting the central nervous system.

(a) State **two** effects, in **each** case, on the body of taking

(i) a low dose of a tranquilizer. *[2]*

. . . .
. . . .
. . . .
. . . .

(ii) a high dose of a sedative. *[2]*

. . . .
. . . .
. . . .
. . . .

(b) Explain why depressants are sometimes described as anti-depressants. *[1]*

. . . .
. . . .

(c) List **two** depressants whose structures are shown in Table 21 of the Data Booklet. *[1]*

. . . .
. . . .

(d) One problem with many drugs is that users develop *tolerance*. Explain what is meant by the term *tolerance* and state why it could increase the risk to the user. *[2]*

. . . .
. . . .
. . . .
. . . .

8804-6103

Figure 11. The watermarked exam

A high degree of similarity between the original and watermarked image is displayed in Table 2. This illustrates the suggested code's great efficiency without changing the exam's original content.

Table 2. The MAE, MSE, PSNR, SSIM, and UIQI of the proposed algorithm

Images: Size/ JPG	**Image Quality Measurements Based on Proposed Approach "LSB"**				
	MAE	**MSE**	**PSNR**	**SSIM**	**UIQI**
2479*3508, 355KB	0.0028	0.00791	69.149	0.99998	0.99998

Table 3. Signal to noise ratio of some of the existing approaches

Techniques	PSNR
Alattar [45]	22.36
Shih and Wu [46]	29.23
Tai et al. [47]	38.0
Yang et al. [48]	29.39
Wang et al. [49]	44.64
Shih et al. [50]	51.24

Another image is used to calculate PSNR. In other words, one image is watermarked, whereas the other is original. A high PSNR suggests that the watermarked image is highly similar to the original. The results in Table 2 made it evident that the suggested method produced a high PSNR.

Table 3 shows a significant discrepancy between PSNR and the suggested model when compared to some other publications. PSNR, however, is effective for comparing intensities. It doesn't offer any structural details. For this reason, picture quality is compared using SSIM or UIQI.

Security of the watermark: because the watermark is dynamic and based on the word information, it protects the watermarked item from both unintentional and intentional attacks, and the watermark signal cannot be retrieved by unauthorized entities.

5. CONCLUSION

In this research paper, a framework has been proposed through which the highest safety standards are achieved in transferring digital images and saving time, cost, and effort.

A crucial aspect of the suggested watermark is its clever and stringent design, which ensures that the watermark is made specifically for each word in an image rather than relying on the image as a whole. Every word has a watermark that includes its location and letter count; ASCII is used to turn the letters into binary information.

The primary advantage of the proposed watermark is that, in the event of manipulation, the original letters can be recovered because the word size is split by the watermark's size. In the recommended method, the original image is not required for watermark verification.

To demonstrate the high similarity between the original image and the watermarked one MSE, PSNR, MAE, UIQI and SSIM are used.

The first step in our proposed algorithm is converting the document's image into text using Optical Character Recognition (OCR), which is one of the limitations of our approach.

In future work, different methods for the OCR will be implemented and utilized instead of the current traditional OCR. The OCR based on AI will replace the traditional OCR. The work will extend not only to finding the areas that have been subjected to deliberations but also to self-correction of changes will be added.

ACKNOWLEDGMENT

This paper was supported by the Korean Agency for Technology and Standard under Ministry of Trade, Industry and Energy in 2023 (Grant No.: K_G012002236201; K_G012002073401; K_G012002234001).

REFERENCES

[1] Al-onazi, B.B., Alotaib, S.S., Alshahrani, S.M., Alotaibi, N., Alnfiai, M.M., Salama, A.S., Hamza, M.A. (2023). Automated Arabic text classification using hyperparameter tuned hybrid deep learning model. Computers, Materials & Continua, 74(3): 5447-5465. https://doi.org/10.32604/cmc.2023.033564

[2] Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G. (1998). Attacks on copyright marking systems. Information Hiding, 218-238. https://doi.org/10.1007/3-540-49380-8_16

[3] Wolfgang, R.B., Podilchuck, C.I., Delp, E.J. (1999). Perceptual watermarks for digital images and video. Proceedings of the IEEE, 87(7): 1108-1126. https://doi.org/10.1109/5.771067

[4] Ghosal, S.K., Mandal, J.K. (2013). Stirling transform based color image authentication. Procedia Technology, 10: 95-104. https://doi.org/10.1016/j.protcy.2013.12.341

[5] Gola, K.K., Gupta, B., Iqbal, Z. (2014). Modified RSA digital signature scheme for data confidentiality. International Journal of Computer Applications, 106(13). https://doi.org/10.5120/18579-9848

[6] Yong, P.E.N.G., Wei, Z.H.A.O., Feng, X.I.E., Dai, Z.H., Yang, G.A.O., Chen, D.Q. (2012). Secure cloud storage based on cryptographic techniques. The Journal of China Universities of Posts and Telecommunications, 19: 182-189. https://doi.org/10.1016/S1005-8885(11)60424-X

[7] Salavi, R.R., Math, M.M., Kulkarni, U.P. (2019). A survey of various cryptographic techniques: From traditional cryptography to fully homomorphic encryption. Innovations in Computer Science and Engineering, 295-305. https://doi.org/10.1007/978-981-13-7082-3_34

[8] Sultan, K., Aldhafferi, N., Alqahtani, A., Mahmud, M. (2018). Reversible and fragile watermarking for medical images. Computational and Mathematical Methods in Medicine, 2018: 3461382. https://doi.org/10.1155/2018/3461382

[9] Balasamy, K., Shamia, D. (2023). Feature extraction-based medical image watermarking using fuzzy-based median filter. IETE Journal of Research, 69(1): 83-91. https://doi.org/10.1080/03772063.2021.1893231

[10] Chen, C.C., Chang, C.C., Lin, C.C., Su, G.D. (2019). TSIA: A novel image authentication scheme for AMBTC-based compressed images using turtle shell based reference matrix. IEEE Access, 7: 149515-149526. https://doi.org/10.1109/ACCESS.2019.2944833

[11] Dhole, V.S., Patil, N.N. (2015). Self embedding fragile watermarking for image tampering detection and image recovery using self recovery blocks. In 2015 International Conference on Computing Communication Control and Automation, Pune, India, pp. 752-757. https://doi.org/10.1109/ICCUBEA.2015.150

[12] Fridrich, J., Goljan, M. (1999). Images with self-correcting capabilities. In Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348), Kobe, Japan, pp. 792-796. https://doi.org/10.1109/ICIP.1999.817228

[13] Ghosal, S.K., Mandal, J.K. (2014). Binomial transform based fragile watermarking for image authentication. Journal of Information Security and Applications, 19(4-5): 272-281. https://doi.org/10.1016/j.jisa.2014.07.004

[14] Gul, E., Ozturk, S. (2019). A novel hash function based

fragile watermarking method for image integrity. Multimedia Tools and Applications, 78: 17701-17718. https://doi.org/10.1007/s11042-018-7084-0

[15] Lee, T.Y., Lin, S.D. (2008). Dual watermark for image tamper detection and recovery. Pattern Recognition, 41(11): 3497-3506. https://doi.org/10.1016/j.patcog.2008.05.003

[16] Li, W., Lin, C.C., Pan, J.S. (2016). Novel image authentication scheme with fine image quality for BTC-based compressed images. Multimedia Tools and Applications, 75: 4771-4793. https://doi.org/10.1007/s11042-015-2502-z

[17] Lin, C.C., Huang, Y.H., Tai, W.L. (2014). A high-quality image authentication scheme for AMBTC-compressed images. KSII Transactions on Internet and Information Systems (TIIS), 8(12): 4588-4603. https://doi.org/10.3837/tiis.2014.12.020

[18] Lin, C.C., Huang, Y.H., Tai, W.L. (2017). A novel hybrid image authentication scheme based on absolute moment block truncation coding. Multimedia Tools and Applications, 76: 463-488. https://doi.org/10.1007/s11042-015-3059-6

[19] Ramakrishnan, S., Gopalakrishnan, T., Balasamy, K. (2011). A wavelet based hybrid SVD algorithm for digital image watermarking. Signal & Image Processing, 2(3): 157-174. https://doi.org/10.5121/sipij.2011.2313

[20] Qin, C., Wang, H.L., Zhang, X.P., Sun, X.M. (2016). Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode. Information Sciences, 373: 233-250. https://doi.org/10.1016/j.ins.2016.09.001

[21] Qin, C., Ji, P., Zhang, X.P., Dong, J., Wang, J.W. (2017). Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy. Signal Processing, 138: 280-293. https://doi.org/10.1016/j.sigpro.2017.03.033

[22] Singh, D., Shivani, S., Agarwal, S. (2013). Self-embedding pixel wise fragile watermarking scheme for image authentication. Intelligent Interactive Technologies and Multimedia, 111-122. https://doi.org/10.1007/978-3-642-37463-0_10

[23] Su, G.D., Chang, C.C., Lin, C.C. (2019). High-precision authentication scheme based on matrix encoding for AMBTC-compressed images. Symmetry, 11(8): 996. https://doi.org/10.3390/sym11080996

[24] Yang, C.W., Shen, J.J. (2010). Recover the tampered image based on VQ indexing. Signal Processing, 90(1): 331-343. https://doi.org/10.1016/j.sigpro.2009.07.007

[25] Zhang, X.P., Wang, S.Z. (2008). Fragile watermarking with error-free restoration capability. IEEE Transactions on Multimedia, 10(8): 1490-1499. https://doi.org/10.1109/TMM.2008.2007334

[26] Zhang, X.P., Wang, S.Z., Feng, G.R. (2009). Fragile watermarking scheme with extensive content restoration capability. Digital Watermarking: 268-278. https://doi.org/10.1007/978-3-642-03688-0_24

[27] Zhang, X.P., Wang, S.Z., Qian, Z.X., Feng, G.R. (2010). Reference sharing mechanism for watermark self-embedding. IEEE Transactions on Image Processing, 20(2): 485-495. https://doi.org/10.1109/TIP.2010.2066981

[28] Zhang, H., Wang, C., Zhou, X. (2017). Fragile watermarking for image authentication using the characteristic of SVD. Algorithms, 10(1): 27. https://doi.org/10.3390/a10010027

[29] Zhu, X.Z., Ho, A.T., Marziliano, P. (2007). A new semi-fragile image watermarking with robust tampering restoration using irregular sampling. Signal Processing: Image Communication, 22(5): 515-528. https://doi.org/10.1016/j.image.2007.03.004

[30] Ahvanooey, M.T., Li, Q., Zhu, X.F., Alazab, M., Zhang, J. (2020). ANiTW: A novel intelligent text watermarking technique for forensic identification of spurious information on social media. Computers & Security, 90: 101702. https://doi.org/10.1016/j.cose.2019.101702

[31] Chen, T.H., Horng, G., Lee, W.B. (2005). A publicly verifiable copyright-proving scheme resistant to malicious attacks. IEEE Transactions on Industrial Electronics, 52(1): 327-334. https://doi.org/10.1109/TIE.2004.841083

[32] Chang, C.C., Lin, P.Y. (2008). Adaptive watermark mechanism for rightful ownership protection. Journal of Systems and Software, 81(7): 1118-1129. https://doi.org/10.1016/j.jss.2007.07.036

[33] Szyller, S., Atli, B.G., Marchal, S., Asokan, N. (2021). Dawn: Dynamic adversarial watermarking of neural networks. In Proceedings of the 29th ACM International Conference on Multimedia, pp. 4417-4425. https://doi.org/10.1145/3474085.3475591

[34] Lu, Z.M., Guo, S.Z. (2016). Lossless Information Hiding in Images. Syngress.

[35] Abdallah, M.S. Cho, Y.I. (2022). Virtual hairstyle service using GANs & segmentation mask (hairstyle transfer system). Electronics, 11(20): 3299. https://doi.org/10.3390/electronics11203299

[36] Hosny, K.M., Darwish, M.M., Fouda, M.M. (2021). New color image zero-watermarking using orthogonal multi-channel fractional-order legendre-fourier moments. IEEE Access, 9: 91209-91219. https://doi.org/10.1109/ACCESS.2021.3091614

[37] Farfoura, M.E., Horng, S.J., Wang, X. (2013). A novel blind reversible method for watermarking relational databases. Journal of the Chinese Institute of Engineers, 36(1): 87-97. https://doi.org/10.1080/02533839.2012.726041

[38] Mishra, A., Jain, A., Narwaria, M., Agarwal, C. (2011). An experimental study into objective quality assessment of watermarked images. In International Journal of Image Processing, 5(2): 199-219.

[39] Abdel-Aziz, B., Chouinard, J.Y. (2004). On perceptual quality of watermarked images – an experimental approach. Digital Watermarking, 277-288. https://doi.org/10.1007/978-3-540-24624-4_21

[40] Kutter, M., Petitcolas, F. (1999). Fair benchmark for image watermarking systems. In Proceedings of SPIE Conference on Security and Watermaking of Multimedia Contents, SPIE, 3657: 226-239. https://doi.org/10.1117/12.344672

[41] Cox, I.J., Miller, M.L. (2002). The first 50 years of electronic watermarking. EURASIP Journal on Advances in Signal Processing, 2002: 820936. https://doi.org/10.1155/S1110865702000525

[42] Abdallah, M.S., Cho, Y.I. (2022). Virtual hairstyle service using GANs & segmentation mask (hairstyle transfer system). Electronics, 11(20): 3299. https://doi.org/10.3390/electronics11203299

[43] Poonam, Arora, S.M. (2018). A DWT-SVD based robust digital watermarking for digital images. Procedia

Computer Science, 132(C): 1441-1448. https://doi.org/10.1016/j.procs.2018.05.076

[44] Kadian, P., Arora, N., Arora, S.M. (2019). March. Performance evaluation of robust watermarking using DWT-SVD and RDWT-SVD. In 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, pp. 987-991. https://doi.org/10.1109/SPIN.2019.8711681

[45] Alattar, A.M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. In IEEE Transactions on Image Processing, 13(8): 1147-1156. https://doi.org/10.1109/TIP.2004.828418

[46] Shih, F.Y., Wu, Y.T. (2005). Robust watermarking and compression for medical images based on genetic algorithms. Information Sciences, 175(3): 200-216. https://doi.org/10.1016/j.ins.2005.01.013

[47] Tai, W.L., Yeh, C.M., Chang, C.C. (2009). Reversible data hiding based on histogram modification of pixel differences. IEEE Transactions on Circuits and Systems for Video Technology, 19(6): 906-910. https://doi.org/10.1109/TCSVT.2009.2017409

[48] Yang, B., Schmucker, M., Funk, W., Busch, C., Sun, S. (2004). Integer DCT-based reversible watermarking for images using companding technique. In Security, Steganography, and Watermarking of Multimedia Contents VI, San Jose, California, USA, pp. 405-415. https://doi.org/10.1117/12.527216

[49] Wang, J.X., Ni, J.Q., Zhang, X., Shi, Y.Q. (2016). Rate and distortion optimization for reversible data hiding using multiple histogram shifting. IEEE Transactions on Cybernetics, 47(2): 315-326. https://doi.org/10.1109/TCYB.2015.2514110

[50] Shih, F.Y., Zhong, X. (2016). High-capacity multiple regions of interest watermarking for medical images. Information Sciences: An International Journal, 367(C): 648-659. https://doi.org/10.1016/j.ins.2016.07.015