A New Face Image Authentication Scheme based on Bicubic Interpolation

Muntadher H. Al-Haddad[*], Rasha Thabit[**], Khamis A. Zidan[***]

[*] Department of Computer Engineering, Al-Iraqia University, Baghdad, Iraq
Email: muntazir3haydar@gmail.com
https://orcid.org/0009-0004-3764-2768

[**] Department of Computer Engineering, Al-Iraqia University, Baghdad, Iraq
Email: rasha.thabit@aliraqia.edu.iq
https://orcid.org/0000-0003-4141-5723

[***] Vice Rector of Al-Iraqia University for Scientific Affairs, Al-Iraqia University, Baghdad, Iraq
Email: khamis_zidan@aliraqia.edu.iq
https://orcid.org/0000-0002-3739-7270

Abstract

Nowadays, image manipulation algorithms are increasingly being used even by people who do not have any deep knowledge of technology, and one can easily find an application to manipulate face image for various purposes. After the development of image processing algorithms, the research community highlighted the need to develop a technology that detects image manipulation, but it did not highlight the recovery of the facial region after manipulation localization, which would be very useful in practical applications. In this paper, a new face image modification detection and recovery scheme based on image watermarking and bicubic interpolation algorithm is presented. Several experiments were conducted to evaluate the performance of the proposed scheme, which proved its effectiveness in generating high-quality watermarked images, detecting different types of manipulation, localizing the manipulated blocks in the face region, and restoring the face region with good visual quality. A comparison with the latest detection techniques demonstrates the superiority of the proposed scheme**.**

Keywords- Bicubic interpolation, Face image manipulation detection, DeepFakes, watermarking image.

I. INTRODUCTION

In recent years, technological advancements have increased the sharing of digital images via internet in almost all fields, as it has become an essential part of many businesses to overcome distance constraints, test different systems and documentation processes, share memories, and others. Since these images are shared through the internet, these images are exposed to manipulation by individuals or institutions [1], [2]. In late 2017, the term 'DeepFakes' was used to refer to an algorithm that was used to transfer celebrity faces into pornographic movies [3]. Later, the term 'DeepFakes' was coined to describe facial image alteration algorithms based on Machine-Learning (ML) and Deep Learning (DL) algorithms [4], [5].

Face image manipulations can be classified into two types. The first type called malicious attacks in which images are manipulated for malicious purposes such as extortion, defamation, and dissemination of false news [6]–[8]. The second type called harmless attacks in which manipulation is applied for good intentions such as facial beautification, adding funny stickers, hair coloring and others. Although the intentions are different in both cases, both cases are considered facial image manipulation. Given the seriousness of malicious attacks on human privacy and their categorization as cybercrimes accountable under the law, researchers have increasingly sought ways to detect manipulation to preserve privacy and preserve facts from manipulation [9]–[11].

Many algorithms have emerged to detect facial manipulation and detect whether an image is intact or has been manipulated [11]–[13]. However, the previous methods suffered from several problems that can be summarized in the following points:

- Previous techniques required large sets of high-quality data for training purposes [14], [15].
- The need for knowing the type of manipulation applied in order to choose the suitable detection technique [16]–[18].
- The high complexity and time-consuming process required for training networks [19].
- Generating high-quality fake face images that are difficult for the trained network to detect [20].

The available detection techniques cannot recover the face region if manipulations are detected. The possibility of retrieving the tampered part upon detection of tampering will be very useful in the field of facial image authentication, especially in the fields of military and forensic analysis. To overcome the limitations and to provide the ability to recover the original face region after manipulation detection. This paper presents a new face image authentication scheme based on image watermarking and bicubic interpolation. According to the practical experiments that were conducted, it was found that the bicubic method gave the greatest results, Compared with the detection and recovery system. The contributions of this research can be summarized as follows:

- Counter to most of the previous techniques, which can only detect one form of manipulation, the proposed system can detect many types of facial image manipulation.
- The proposed scheme has the ability to recovery the image of the original face upon detection of tampering, while previous techniques did not address this idea.
- The ability of localizing manipulations while most of the available schemes cannot localize the manipulated region.
- Counter to previous techniques that depend on deep learning and that require large data sets for training, the proposed scheme does not need training at all.

The rest of the article offers the suggested algorithms in the second section, samples of the experimental findings and their discussion in the third section, and finally the research conclusions in the fourth section.

II. RESEARCH ELABORATIONS

The suggested approach is made up of two major algorithms: embedding and extraction algorithms. The manipulation localization and recovery information are created from the face region and embedded in the area outside the face region on the embedding side. The embedded information is collected from the area outside the face region and utilized for localizing manipulations and recovering the face region if manipulations occur which is performed on the extraction side. The recovery information from face region are generated using bicubic interpolation algorithm. The details of the proposed algorithm are explained in the following subsections which are applied from two aspects as follows:

A. Proposed bicubic based embedding algorithm.

The proposed embedding algorithm is applied at the sender side in which the input is the original face image $I_f(M \times N \times 3)$ and the output is the watermarked face image $I_w(M \times N \times 3)$ where M is the height and N is the width of the image. The details of the algorithm are explained in four stages:

- ***Stage 1*:** In this stage, the original image is being read and the face region is identified using Multi-Task Cascaded Convolution Neural Networks (MTCNN) algorithm [14]. As shown in Figure 1. The block diagram of stage 1 is shown in Figure 2 and the details of the algorithm are explained as follows :

1. Read the input image $I_f(M \times N \times 3)$.
2. Apply MTCNN algorithm to detect face window, the output of this step is modified to select the pixels of the face region.
3. Generate black and white (BW) image of size (M×N) in which the pixels at the face window are set to ones and the others are set to zeros as shown in Figure 1.
4. Apply bicubic interpolation with scale value (0.5).
5. Select one channel from the face region and convert it to binary then concatenate the binary bits to obtain one binary sequence.
6. Repeat step 5 to the remaining two channels and calculate the length of the resultant binary sequences.

Figure 1: Detect the face window and generate BW image.

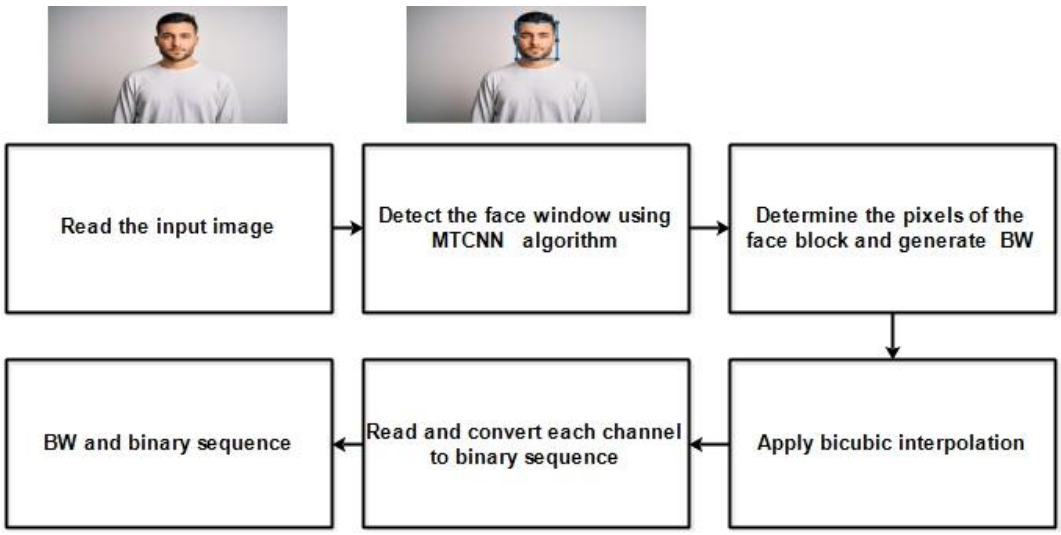

Figure 2: Stage 1 of the proposed bicubic based embedding algorithm.

- *Stage 2*: In this stage, the I_f and BW images are considered as inputs, the block diagram of the stage 2 is shown in Figure 3. Each channel image is divided into non-overlapping blocks of size (16 x 16) pixels. The same process is applied to BW, and then the blocks of BW are averaged to classify the channel blocks into two groups of face area blocks and non-face blocks. When the average of the BW block is not equal to zero, the channel block at the same position is classified as the block of the face area, otherwise the block belongs to the group of non-face blocks.

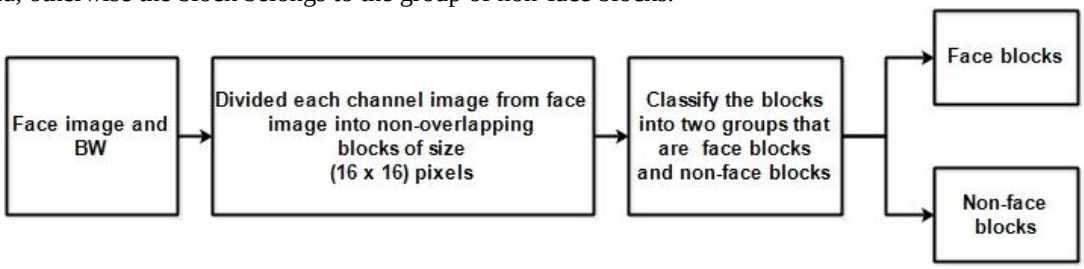

Figure 3: Stage 2 for the proposed bicubic based embedding algorithm.

- *Stage 3*: In this stage, face blocks are the input to generate the localization data. The block diagram of this stage is shown in Figure 4. And the details of the algorithm are explained as follows: Attend conferences, workshops and symposiums on the same fields or on related counterparts.

1. To generate the localization data the value of each face block that connects to the resulting binary face region sequence from stage 1 is averaged.
2. The resulting binary sequences are then connected to form a single binary sequence. BCH (11,15,1).
3. Modify coefficients to carry the binary sequence.

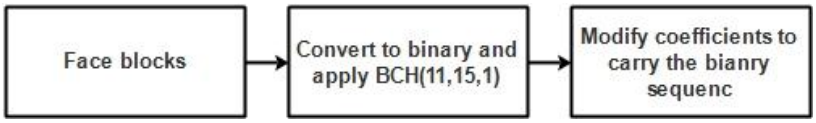

Figure 4: Stage 3 for the proposed bicubic based embedding algorithm.

- *Stage 4*: In this stage, the non-face blocks are input for this stage. The block diagram of this stage is shown in Figure 5. And the details of the algorithm are explained as follows:

1. The non-face blocks transformed using the SLT matrix of size (16×16) as follows:

$$T_{non\text{-}face\_Block} = [SLT_{16}]\ [\text{non-face\_Block}]\ [SLT_{16}{}^{T}]$$

where $T_{non\text{-}face\_Block}$ refers to the transformed non-face_Block, SLT_{16} refers to SLT matrix of size (16×16), and $SLT_{16}{}^{T}$ refers to the transpose of SLT_{16}.

2. Then the resulting SLT coefficients are divided into 4 subsequent (i.e., HH, HL, LH, and LL).
3. Subsequent result is included in subbands (HL and LH) of the SLT using the watermark embedding rules that were applied to the non-facet blocks.
4. After applying the inverse SLT transform to get the non-face watermarked blocks.

5. Then construct the watermarked channel image from the face blocks and the non-face watermarked blocks.
6. The steps are repeated to obtain the second and third channels with the watermarked face image, and create Watermark the I_w face image from the output watermarked channels.

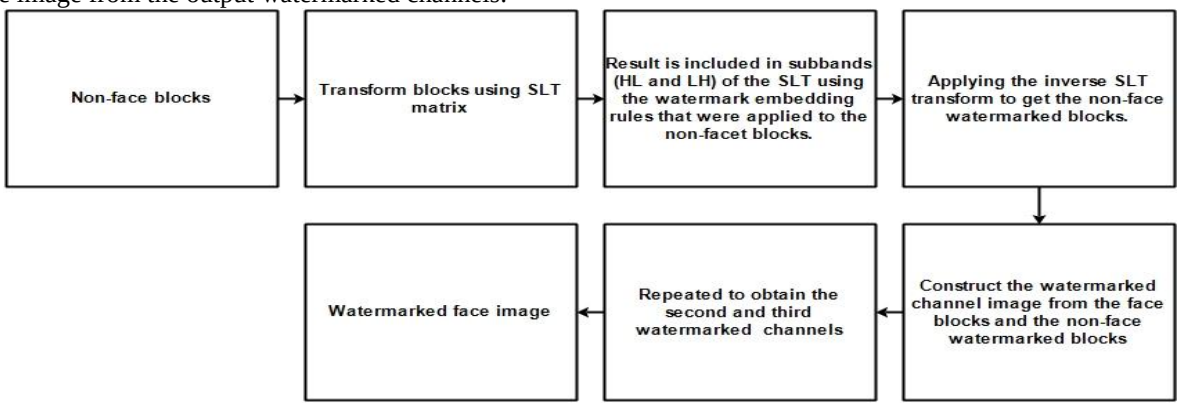

Figure 5: Stage 4 for the proposed bicubic based embedding algorithm.

B. Proposed bicubic based extraction algorithm

The suggested extraction technique is used at the receiver side, with the watermarked face picture as input and the result of face image authentication as output. The details of algorithm are explained in three stages:

- *Stage 1*: In this stage, the input of this algorithm is watermarked face image. The block diagram of this stage is shown in Figure 6. And the steps of this algorithm are as follows:

1. The watermarked channel image and the mask image will be read.
2. Apply MTCNN to detect the face box. As a result of this step is done select the pixels of face blocks and generated BW.
3. After read one channel from input face image, the channel image and mask image will be divided into non-overlapping blocks of size (16×16). The same procedure at the embedding side is repeated in this stage.
4. The average of mask image blocks will be calculated and the channel blocks will be classified into two groups called face blocks and non-face blocks, The mean of the face blocks will be calculated and save them for later comparison steps.

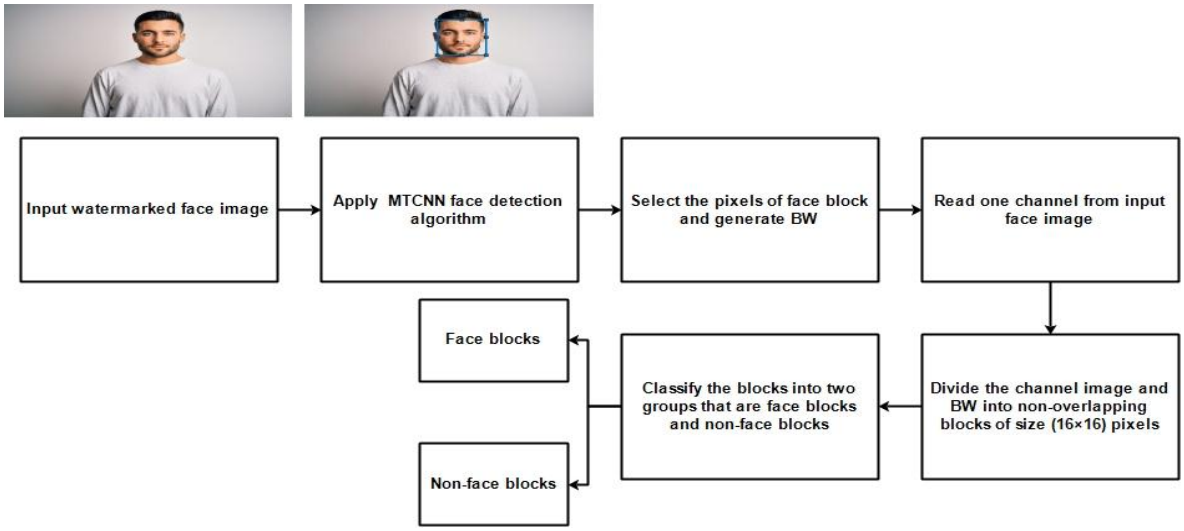

Figure 6: Stage 1 for the proposed bicubic based extraction algorithm.

- *Stage 2*: This stage is divided into two parts. In part 1, calculate average for each block in face block for compare extracted and calculate data for used later, in part 2, the non-face blocks are the input for this stage and transformed it using the SLT matrix of size (16×16). As shown in Figure 7, the steps of this algorithm are as follows:

1. Transformed the non-face blocks are using the SLT matrix of size (16×16). The same procedure at the embedding side is repeated in this stage.
2. The data extraction algorithm is applied in this stage to extract the binary sequence that has been embedded in the blocks outside the face region. The extracted binary sequence is separated into two sub-sequences one for localization and the other one is for recovery.

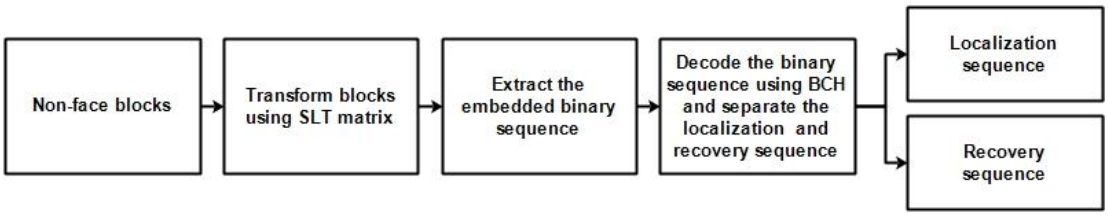

Figure 7: Stage 2 for the proposed bicubic based extraction algorithm.

- *Stage 3*: In this stage data from the first and second stage are used for compare rustle. As shown in Figure 8. And the steps of this stage are as follows:

1. From stage 1, the average values of the facial area masses are calculated.
2. From the binary sequence extracted in stage 2, the mean values are retrieved
3. Compare the extracted and calculated average values to detect manipulations. If the average values for the image block are equal then the block is authentic. If the average values are not equal then the block is considered unauthentic, the block is localized by drawing a border on its pixels and the procedure continues to recover the face region.
4. Repeat the steps to reveal manipulation in the three channels of the watermarked face image.
5. Recovery face region, recovery is explained in the following steps:
   - The binary sequence is read for one channel.
   - Divide the binary sequence into consecutive sequences of (8 bits).
   - Converts subsequent binaries to decimal to recover the resized channel.
   - Repeat the previous steps on the second and third channel.
   - Finally, the bicubic interpolation algorithm with scale value (2) is applied to the retrieved resized face region.

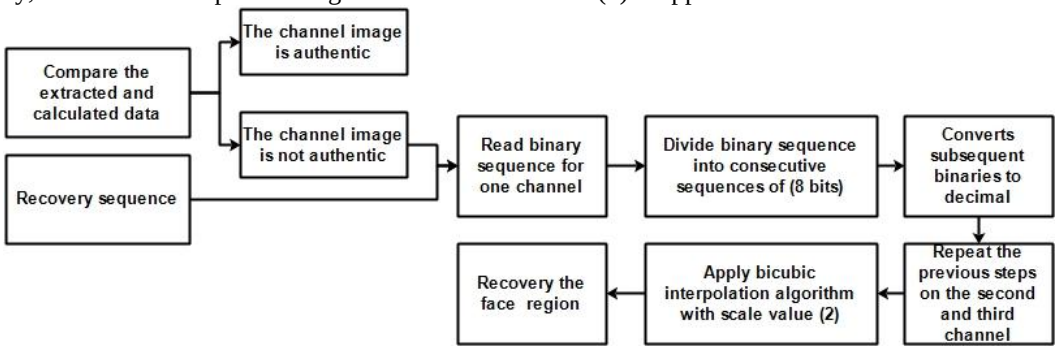

Figure 8: Stage 3 for the proposed bicubic based extraction algorithm.

III. RESULTS AND DISCUSSIONS

To test the performance of the proposed scheme, several experiments were done using different test images. Figure 9 shows sample test images that contain images of different sizes in terms of size of image and size of face area. The following subsections present and discuss the experiments, followed by a general comparison with the most recent schemes to prove the efficiency of the proposed scheme.

Figure 9: Sample test image

A. Capacity and payload test

Capacity refers to the total number of bits that may be stored in the non-face blocks, whereas payload refers to the length of the binary sequence produced from the localization and recovery data. Table 1 shows the results of this experiment for the sample images presented in Figure 9. The results show that the larger the face area, the greater the payload, and vice versa. The capacity is determined by the size of the face area within the image, as the capacity increases as the size of the face decreases relative to the size of the original image, and vice versa.

Table 1: Capacity and payload test results

Image name	Size of the face image	Size of detected face area	Payload (bits)	Capacity (bits)
Img_1	360×540×3	112×80×3	24960	43392
Img_2	408×612×3	112×96×3	29952	57216
Img_3	339 ×509× 3	80 ×64× 3	14336	39744
Img_4	365 ×473× 3	112 ×80 ×3	24960	37760
Img_5	408× 612× 3	96 ×80× 3	21440	58112
Img_6	351×492×3	64 ×48× 3	8640	39040
Img_7	612 ×506× 3	128×112×3	39936	70784
Img_8	339×509×3	128×96×3	34240	37632
Img_9	1667×2500×3	464×384×3	494144	990336
Img_10	742×1320×3	160×128×3	56960	235072

B. Visual quality and time complexity test

The visual quality of the resultant watermarked images has been evaluated using Peak signal-to-noise ratio PSNR in decibel between the original face image and the watermarked image. The time complexity has been calculated for the embedding and extraction algorithms using the tic toc command in MATLAB software.

The computer in this experiment has the following characteristics: Core TM i7 CPU 2.60 GHz Intel® and 8 GB memory. Table 2 displays the findings, which demonstrate the suggested scheme's effectiveness in producing high-visual-quality watermarked image. The time complexity test results demonstrated that the embedding time is less than the extraction time.

Table 2: Visual quality and time complexity test results

Image name	PSNR (dB)	Embedded time (sec.)	Extraction time (sec.)
Img_1	47.232388	0.895500	7.982903
Img_2	48.092879	1.113970	3.524042
Img_3	49.986716	2.962385	218.007269
Img_4	39.185097	2.684002	16.578812
Img_5	49.639893	0.870363	7.450810
Img_6	42.850258	1.133967	16.639052
Img_7	47.562535	0.778159	2.038819
Img_8	42.581882	3.587124	24.023276
Img_9	46.024388	0.831364	5.83066
Img_10	45.87782	1.008750	15.998195

C. Face manipulation localization and recovery

Watermarked facial images were manipulated using various attacks such as retouching, attribute attacks, face swaps, expression swaps, and morphing to test the proposed scheme's ability to detect facial area manipulations and restore the original facial area when manipulations are present. Sample findings are provided in Figure 10 to Figure 12, demonstrating that the proposed approach can localize the altered region and restore the original face region regardless of its size.

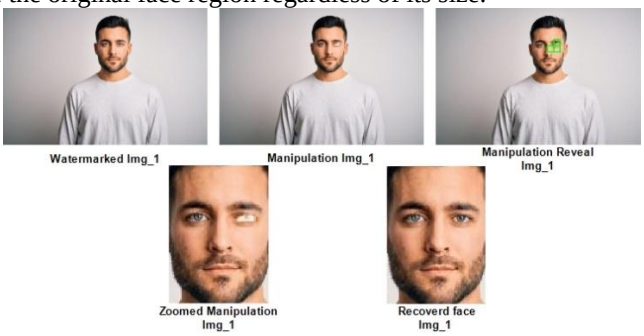

Figure 10: Manipulation localization and recovery attributes attack of test image ‘Img_1’.

Figure 11: Manipulation localization and recovery expression swap of test image 'Img_2'.

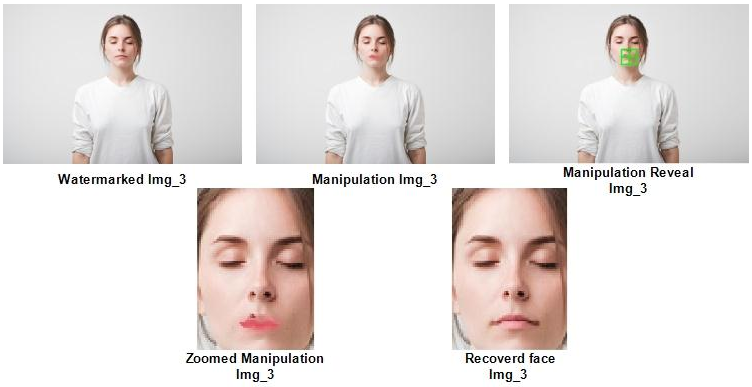

Figure 12: Manipulation localization and recovery retouching attack of test image 'Img_3'.

D. Comparison with the state-of-the-art schemes

Because it can detect multiple sorts of manipulations, localize the manipulated blocks in the face area, and restore the face region if manipulations exist, the proposed scheme outperforms many state-of-the-art approaches. Table 3 compares the proposed scheme to different facial image modification detection algorithms in general.

Table 3: General comparison of the proposed scheme with state-of-the-art

Scheme	**Method**	**Various manipulations**	**Manipulation detection**	**Block based localization**	**Face region recovery**
[8], [11]	Deep-learning	×	✓	×	×
[13]	Watermarking	✓	✓	✓	×
Proposed	Watermarking + Bicubic interpolation	✓	✓	✓	✓

IV. CONCLUSION

Recently, researchers have shed light on the technique of detecting facial manipulation. Different algorithms have been presented, but they did not address the retrieval of the face image after detecting and localization the manipulation. This paper proposes a new practical method for face image authentication through image retrieval of tampered face after detection and localization of tampering using bicubic interpolation algorithm. The image is divided into non-overlapping blocks of size (16 x 16) pixels. as a result of the partitioning process, the blocks are classified into face blocks and non-face blocks based on the result of the face detection and selection process. With watermark embedding technology, tamper detection information is generated from face blocks embedded in non-face blocks. To gauge performance, pilot tests were run. The suggested technique is efficient at finding various forms of tampering. After tampering has been identified and localized, the ability of the scheme to recover the manipulated part. Thus, the proposed scheme is distinguished from previous schemes that operate in this field.

ACKNOWLEDGMENT

The authors extend their thanks to Al-Iraqia University for supporting this research.

REFERENCES

[1] J. M. Zain and A. R. M. Fauzi, "Medical image watermarking with tamper detection and recovery", in 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, IEEE, 2006, pp. 3270–3273.

[2] J. M. Zain and A. R. M. Fauzi, "Evaluation of medical image watermarking with tamper detection and recovery (AW-TDR)", in 2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, IEEE, 2007, pp. 5661–5664.

[3] B. Bitesize, "Deepfakes: what are they and why would i make one", BBC Bitesize Articles, 2019. [Online]. Available: https://www.bbc.co.uk/bitesize/articles/zfkwcqt

[4] J. Kietzmann, L. W. Lee, I. P. McCarthy, and T. C. Kietzmann, "Deepfakes: Trick or treat?", Bus Horiz, vol. 63, no. 2, pp. 135–146, 2020, https://doi.org/10.1016/j.bushor.2019.11.006.

[5] M. M. Waldrop, "Synthetic media: The real trouble with deepfakes", Knowable Magazine, Mar. 2020, 10.1146/KNOWABLE-031320-1/FEATURE/MEDIA/G-NEURAL-NETWORK-MODEL.SVG.

[6] M. Kulkarni and Mr. R. T. Patil, "Tamper Detection & Recovery in Medical Image with secure data hiding using Reversible watermarking", 2012.

[7] A. M. Almars, "Deepfakes Detection Techniques Using Deep Learning: A Survey", Journal of Computer and Communications, vol. 09, no. 05, 2021, 10.4236/jcc.2021.95003.

[8] F. Matern, C. Riess, and M. Stamminger, "Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations", in 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW), 2019, pp. 83–92. 10.1109/WACVW.2019.00020.

[9] S. Fadnavis, "MicroLearn: Framework for machine learning, reconstruction, optimization and microstructure modeling View project Image Interpolation Techniques in Digital Image Processing: An Overview", 2014. [Online]. Available: www.ijera.com

[10] Z. A. Salih, R. Thabit, K. A. Zidan, and B. E. Khoo, "Challenges of Face Image Authentication and Suggested Solutions", in 2022 International Conference on Information Technology Systems and Innovation, ICITSI 2022 - Proceedings, 2022. 10.1109/ICITSI56531.2022.9970797.

[11] H. Li, B. Li, S. Tan, and J. Huang, "Detection of Deep Network Generated Images Using Disparities in Color Components", ArXiv, vol. abs/1808.0, 2018.

[12] R. Thabit and B. E. Khoo, "Medical image authentication using SLT and IWT schemes", Multimed Tools Appl, vol. 76, no. 1, pp. 309–332, Jan. 2017, doi: 10.1007/s11042-015-3055-x.

[13] Z. A. Salih, R. Thabit, K. A. Zidan, and B. E. Khoo, "A new face image manipulation reveal scheme based on face detection and image watermarking", in 2022 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET), 2022, pp. 1–6. doi: 10.1109/IICAIET55139.2022.9936838.

[14] R. Thabit and B. E. Khoo, "Capacity improved robust lossless image watermarking", IET Image Process, vol. 8, no. 11, pp. 662–670, Nov. 2014, 10.1049/iet-ipr.2013.0862.

[15] [13] Z. A. Salih, R. Thabit, K. A. Zidan, "A new manipulation detection and localization scheme for digital face images," J. Eng. Sci. Technol., vol. 18, no. 2, pp. 1164–1183, 2023, [Online]. Available: https://jestec.taylors.edu.my/Vol 18 Issue 2 April 2023/18_2_21.pdf

[16] S. H. Silva, M. Bethany, A. M. Votto, I. H. Scarff, N. Beebe, and P. Najafirad, "Deepfake forensics analysis: An explainable hierarchical ensemble of weakly supervised models", Forensic Sci Int, vol. 4, p. 100217, 2022, https://doi.org/10.1016/j.fsisyn.2022.100217.

[17] S. Kolagati, T. Priyadharshini, and V. Mary Anita Rajam, "Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model", International Journal of Information Management Data Insights, vol. 2, no. 1, p. 100054, 2022, https://doi.org/10.1016/j.jjimei.2021.100054.

[18] R. Thabit and B. E. Khoo, "Robust reversible watermarking scheme using Slantlet transform matrix", Journal of Systems and Software, vol. 88, no. 1, 2014, 10.1016/j.jss.2013.09.033.

[19] R. Walia, "Zooming Digital Images using Modal Interpolation International Journal of Application or Innovation in Engineering & Management (IJAIEM)", 2013. [Online]. Available: https://www.researchgate.net/publication/274702043

[20] Z. A. Salih, R. Thabit, K. A. Zidan, and B. E. Khoo, "A new face image manipulation reveal scheme based on face detection and image watermarking", in 4th IEEE International Conference on Artificial Intelligence in Engineering and Technology, IICAIET 2022, 2022. 10.1109/IICAIET55139.2022.9936838.