# **Video Copyright Protection**

https://doi.org/10.3991/ijim.v17i08.39339

Muna Majeed Laftah<sup>(⊠)</sup>, Iman I. Hamid, Nashwan Alsalam Ali University of Baghdad, Baghdad, Iraq muna.majeed@coeduw.uobaghdad.edu.iq

Abstract-Illegal distribution of digital data is a common danger in the film industry, especially with the rapid spread of the Internet, where it is now possible to easily distribute pirated copies of digital video on a global scale. The Watermarking system inserts invisible signs to the video content without changing the content itself. The aim of this paper is to build an invisible video watermarking system with high imperceptibility. Firstly, the watermark is confused by using the Arnold transform and then dividing into equal, non-overlapping blocks. Each block is then embedded in a specific frame using the Discrete Wavelet Transform (DWT), where the HL band is used for this purpose. Regarding the method of selecting the host frames, the chaotic map (tent map) was used to choose a number of frames which are greater or equal to the number of blocks of the watermark. The host frame selection method makes the discovery of the watermark information by illegal means very complicated. The experimental results show that the proposed method can produce excellent transparency with robustness against some attacks where the average PSNR reaches to 72.806.

Keywords-copyright, chaotic map, Discrete Wavelet Transform, watermark

### 1 Introduction

Presently, images and videos are the main means of information sharing in the modern digital age. The ease with which digital multimedia may be expressed, distributed, and stored makes it possible for information to be transferred, especially with the development of communication devices and information technology [1-3]. Even though there are stringent laws against Cam cording in many nations, it has not been feasible to stop this activity due to these laws' ineffectiveness. In spite of a carefully thought-out anti-piracy operation undertaken by the Warner Brothers studio, more than seven million illicit copies of the Batman movie "The Dark Knight" were downloaded in the first six months after its release, demonstrating the seriousness of this criminal behavior [4-5]. Digital watermarking is a method for concealing a message that may be identified by many types of electrical signals., such as images, sounds, and videos, within the sign itself [6-7]. From the dawn of programming, watermarks have been used to ensure the privacy of data using a variety of means, including audio, text, image watermarks and video. The purpose of the watermark is to identify the true owner of the movie by their personality [8-9]. Watermarking uses the

spatial domain and frequency domain approaches [10]. The frequency domain's methods, often called to as the transform domain's, are more reliable when compared to the spatial domain [11]. Many of the current video watermarking techniques embed the watermark image into every frame of the movie. As a result, attackers will have an easier time identifying frames that conceal the watermark, and the video's storage capacity will also grow [12].

# 2 Related work

A 1-level 2D-DWT is used to transform the Y component of each frame, after which the LH and HL sub-bands were chosen. The result of this, 2D-DCT is used, although in a different frame, on certain sub-bands. Following then, the arrangement was changed using a zigzag scan. A watermark is then added to the middle-frequency coefficient. The watermarked video's PSNR values were around 37 dB based on the testing outcomes of the suggested technique. It has been shown that the suggested method resists HEVC stream compression [13]. A non-blind technique using the singular value decomposition (SVD) and discrete cosine transform (DCT) algorithms was another scheme. In this study, the coefficients of DCT for each frame of the host video are rearranged using zigzag patterns, and the rearranged DCT coefficients are then divided into four blocks. Frequency bands make up these blocks (LL, HL, LH and HH). As a consequence, each block is subjected to SVD independently. In order to get a video watermark, in every block, the singular values are finally updated by the unique DCT watermark image values. The suggested technique is more transparent and attack-resistant, according to experiment results [14]. The proposed a watermark embedding adaptive area selection method. Initially, using a model of saliencybased visual attention, they distinguished between salient and non-salient areas (MSVA). After that, the non-salient regions were divided into blocks, and the texture complexity of each block was calculated. The watermark embedding block was then used, with a small dispersion of image texture complexity. Due to more precisely defined saliency zones, safe watermark embedding, and a decrease in the removal attack on watermark images, the proposed method provided more significant benefits [15].

# **3** Theoretical background

#### 3.1 Wavelet transform

The Straightforward wavelet transform example is the Haar wavelet transform. The image signal is divided into regions using the Haar transform, where one area includes big numbers (in the case of the Haar transform, averages), while the other regions contain tiny numbers (differences) [16]. The subscript behind L and H denotes low frequency and high frequency, respectively, and the total number of layers of the transforms. The mid-frequency and high-frequency detail sub-bands LH, HL,

and HH indicate vertical edge, horizontal edge, and diagonal edge features, respectively. The original video is approximated with a lower resolution in the LL sub-band. The following Equations illustrate how to use the Haar filter to determine each subband coefficients (1), (2), (3), and (4) [17,18]:

$$LL(r,c) = \frac{I(r,c) + I(r,c+1) + I(r+1,c) + I(r+1,c+1)}{2}$$
(1)

$$LH(r,c) = \frac{I(r,c) + I(r,c+1) - I(r+1,c) - I(c+1,c+1)}{2}$$
(2)

$$HL(r,c) = \frac{I(r,c) - I(r,c+1) + I(r+1,c) - I(r+1,c+1)}{2}$$
(3)

$$HH(r,c) = \frac{I(r,c) - I(r,c+1) + I(r+1,c) - I(r+1,c+1)}{2}$$
(4)

where, I: original image, r: width of image, c: length of image.

For achieve decompositions for multi-level, the procedure can be applied many times.

#### 3.2 The Arnold transforms

Chaotic maps are particularly useful tools with a broad range of applications in the field of digital image encryption, due to their unique characteristics, including the periodicity, sensitivity of the initial condition, and their non-periodicity [13]. The frequently utilized chaotic maps in the field of image encryption is the Arnold transformation. The following equations (5), (6), and (7) for the Arnold transform provide an explanation for 2D inverse transform [19]:

$$\begin{pmatrix} x'\\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1\\ 1 & 2 \end{pmatrix} \begin{pmatrix} x\\ y \end{pmatrix} \pmod{N} \ x, y \in 0, 1, \dots, N-1$$
(5)

In this situation, the pixel value for the original image is represented by (x, y), but scrambled image pixel value denoted by (x', y'). N stands for the size of the image.

It might rewrite the transform as follows:

.

$$\begin{cases} x' = (x+y) \mod N \\ y' = (x+2y) \mod N \end{cases}$$
(6)

The following formula in equation (7) can be applied to generate the reverse Arnold map [14]:

$$\binom{x'}{y'} = \binom{2 \ -1}{-1} \binom{x}{y} \pmod{N} \ x, y \in 0, 1, \dots, N-1$$
(7)

#### 3.3 Tent map

The most recently researched map in a variety of cryptography applications is the Chaotic Tent map. Yoshida et al. researched the chaotic behavior of tent maps, and the equation (8) provides the mathematical description of a tent map. [20].

$$x_{i+1} = f(x_i, \mu) = \frac{f_L(x_i, \mu) = \mu x_i}{f_R(x_i, \mu) = \mu(1-x_i)}, \quad x_i < 0.5$$
(8)

The Tent chaotic function just takes one control argument and produces real values between 0 and 1. where  $xi \in [0,1]$ , for  $i \ge 0$ ,  $\mu \in [0,2]$ ,  $x_0$  is the first situation, and  $\mu$  is a control variable that receives an input of a positive real number. The system orbit is the group of real numbers denoted by  $x_0 \dots x_n$ . The plot of the bifurcation diagram can be utilized to study the behavior of the tent map. The sequence number created via the Tent chaotic map with the control parameter  $\mu$  will be plotted using the bifurcation diagram [21, 22].

### 4 Proposed work

The proposed blind invisible watermarking system have main two stages: First is Embedding process and second is extraction process. Each stage has a proposed equation, the proposed modified HL-band equation (9) used for embedding watermark information and proposed extraction equation (10) used for extract watermark information. Figures 1 and 2 shows block diagrams of each process. The next subsections explain each stage in details.

$$HL(1,1) = - \begin{bmatrix} if m=1 \\ if HL(1,1) \text{ greater than } HL(2,1) \text{ then} \\ HL(1,1) = /(HL(1,1))/+Thr \\ else \\ if (HL(1,1) \text{ less than } HL(2,1)) \text{ then} \\ HL(1,1) = /(HL(1,1)/+Thr \\ HL(2,1) = /(HL(2,1)/*(-1)) \end{bmatrix}$$

$$HL(2,1) = - \begin{bmatrix} if m=0 \\ if HL(2,1) \text{ greater than } HL(1,1) \\ HL(2,1) = /(HL(2,1)/+Thr \\ else \\ if (HL(2,1) \text{ less than } HL(1,1)) \\ HL(2,1) = /(HL(2,1)/+Thr \\ HL(1,1) = /(HL(2,1)/+Thr \\ HL(1,1) = /(HL(1,1)/*(-1)) \end{bmatrix}$$

The proposed threshold is representing by *Thr*, and in a proposed work its value will range between (10 to 25).

Paper-Video Copyright Protection

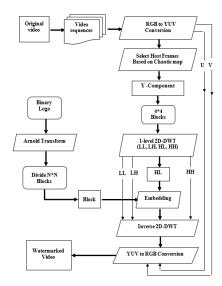


Fig. 1. Embedding process

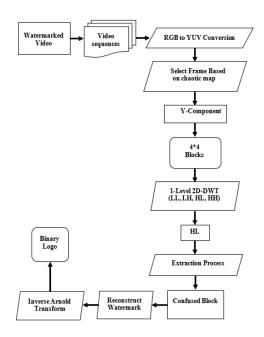


Fig. 2. Extraction Process

#### 4.1 Embedding process

After reading video frames and converting frames from RGB to YCbCr color space, the first primary step of embedding process is select host frames by generating chaotic sequences of number by tent map using equation (8). Second step is dividing watermark image after confuse by Arnold transform using equation (7), into number of N×N blocks and these blocks must be equal or less than number of host frames. Finally, each block inserted in corresponding host frame by following steps.

1. Divide Y component of host frame to 4×4 non-overlapping blocks

2. Apply one level 2D-DWT of each block.

3. Modify HL coefficients by equation (9)

- 4. Apply inverse DWT
- 5. Convert video frames from YCbCr to RGB color space.

#### 4.2 Extraction process

This process starts with reading the video and converting the color space of frames from RGB to YCbCr. Then selecting frames that contain the watermark information by using the tent map with the same key. However, the following several steps comprise the blind watermark information extraction technique:

Divide the Y component into 4x4 blocks without overlapping.

Apply one level 2D-DWT of each block.

- 1. Divide the Y component into 4x4 blocks without overlapping.
- 2. Apply one level 2D-DWT of each block
- 3. Extract watermark block pixel using equation (10)

$$k = \begin{cases} 1 & HL(1, 1) > HL(2, 1) \\ 0 & HL(2, 1) > HL(1, 1) \end{cases}$$
(10)

Finally, reconstruct blocks of confused watermark. And the watermark decryption is implemented using equation (7) by inverse Arnold Transform.

### 5 Results and discussion

As seen in Figure 3, a number of standard videos of type CIF format are used for evaluating the proposed watermarking method. The watermark used is a  $(32 \times 32)$  binary logo. MATLAB 2020 is used for implementing the proposed method. The tests were implemented using Windows 10 on the laptop of Ryzen9 CPU, GPU RTX 3060, and 16G Ram.

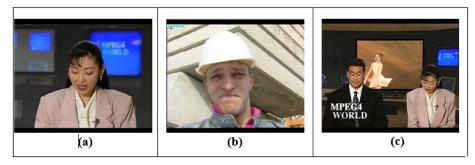


Fig. 3. (a) Akiyo Original frame, (b) Foreman Original frame, (c) News Original frame

#### 5.1 Invisibility tests

In watermarking systems, Invisibility is frequently employed as a measurement of evaluation metric. The invisibility was measured using the PSNR. The PSNR represents how natural the watermarked video will seem to viewers. As seen below, the PSNR can be calculated using equation (11) [23]:

$$PSNR = 10Log10 \frac{255^2}{\frac{1}{w \times h} \sum_{x=1}^{w} \sum_{y=1}^{h} (I_{x,y} - I'_{x,y})^2}$$
(11)

Where the original and watermarked video frames are shown here by the characters I and I', respectively; (x, y) represent the position of a pixel in the original and watermarked frames; and (w, h) represent the original video frame's width and height.

The average PSNR of all watermarked frames may be used to compute the PSNR of a watermarked video [24-34]. The PSNR values for videos with embedded watermarks are shown in Table 1. The better effectiveness of invisibility is indicated by a greater AVPSNR.

$$AV_{PSNR} = \frac{PSNR}{n} \tag{12}$$

Table 1. The PSNR results after the process of embedding

Watermarked video	AV_PSNR
Akiyo	72.806
Foreman	57.079
News	71.808

#### 5.2 Robustness tests

All watermarking techniques must follow to the essential requirement of robustness. It must perform various attacks on the watermarked video to verify robustness, after which it must be evaluate how equivalent the original watermarks and the extracted one by use the bit error (BER) and normal correlation coefficient (NC). The NC and BER are defined using equation (13) and (14) respectively [25, 26, 27]:

$$NC = \frac{\sum_{x=1}^{W} \sum_{j=1}^{L} M(i,j) M'(i,j)}{\sum_{x=1}^{W} \sum_{j=1}^{L} M^{2}(i,j) M'^{2}(i,j)}$$
(13)

M and M' in this instance act the original and extracted watermarks. The W represents the rows and L represents the columns of the watermark.

$$BER = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} w(i,j) \otimes w'(i,j)}{N \times M}$$
(14)

Table 2 results illustrate how the suggested method is resistant to several image processing attacks attempted against watermarked video.

Attack		Akiyo	Foreman	News
No Attack	NC	1	1	1
	BER	0	0	0
Salt & pepper noise (0.01)	NC	0.978	0.962	0.974
	BER	0.005	0.009	0.007
Poisson noise	NC	0.745	0.692	0.648
	BER	0.093	0.114	0.135
Histogram equalization	NC	1	1	1
	BER	0	0	0
Gamma correction	NC	1	0.942	1
	BER	0	0.013	0
Sharpening	NC	1	0.921	1
	BER	0	0.038	0

Table 2. The NC and BER metrics using different attacks for Extracted Watermark

# 6 Conclusion

This work uses a Tent map to pick a specific number of frames. In addition, divide the watermark image into a number of equal blocks, and these blocks must equal or be less than the number of selected host frames. The aim of dividing the watermark is to decrease the effect of embedding on video quality. The proposed method used the Arnold transform for watermark encryption and for the embedding process it used the DWT. These two transformations enhance security and invisibility. The test results show the proposed method has good imperceptibility and robustness against image processing attacks. In addition, the proposed system has some limitations against image compression attacks, which will be solved by adding another transform in the future.

# 7 References

- Thajeel, S.A.-N. and Sulong, G. A novel approach for detection of copy move forgery using completed robust local binary pattern. J Inf Hiding Multimed Signal Process, 6(2): 351-364, 2015.
- [2] N. A. Ali, "Watermarking in 3D Models Using Depth Path", Iraqi Journal of Science, vol. 60, no. 11, pp. 2490–2496, Nov. 2019. <u>https://doi.org/10.24996/ijs.2019.60.11.21</u>
- [3] S. A. Thajeel, "Robust Video Watermarking of Hybrid based techniques", Iraqi Journal of Science, vol. 58, no. 4C, pp. 2458–2466, Jan. 2018. <u>https://doi.org/10.24996/ijs.2017.58.</u> <u>4C.21</u>
- [4] Y. K. Lin, C. H. Yang, and J. T. Tsai, "More secure lossless visible watermarking by DCT," Multimed. Tools Appl., vol. 77, no. 7, pp. 8579–8601, 2018. <u>https://doi.org/10. 1007/s11042-017-4753-3</u>
- [5] M. Saqib and S. Naaz, "Spatial and Frequency Domain Digital Image Watermarking Techniques for Copyright Protection," Int. J. Eng. Sci. Technol., vol. 9, no. 6, pp. 691– 699, 2017.
- [6] K. J. Giri, Z. Jeelani, J. I. Bhat, and R. Bashir, "Survey on Reversible Watermarking Techniques for Medical Images," in Multimedia Security, Springer, 2021, pp. 177–198. <u>https://doi.org/10.1007/978-981-15-8711-5\_9</u>
- [7] B. A. Hameedi, A. A. Hattab, and M. M. Laftah, "A Pseudo-Random Number Generator Based on New Hybrid LFSR and LCG Algorithm", Iraqi Journal of Science, vol. 63, no. 5, pp. 2230–2242, May 2022. <u>https://doi.org/10.24996/ijs.2022.63.5.35</u>
- [8] R. Bala, "A brief survey on robust video watermarking techniques," Int. J. Eng. Sci., vol. 4, no. 2, pp. 41–45, 2015.
- [9] S. Kaur and R. Kaur, "Quality Analysis for Different Video Formats by Using Video Watermarking," Int. J. Eng. Manuf., vol. 6, no. 4, p. 9, 2016. <u>https://doi.org/10.5815/ijem. 2016.04.02</u>
- [10] Ashish M. Kothari, Vedvyas Dwivedi, and Rohit M. Thanki, Watermarking Techniques for Copyright Protection of Videos. 2019. <u>https://doi.org/10.1007/978-3-319-92837-1</u>
- [11] R. Shoitan, M. M. Moussa, and S. M. Elshoura, "A robust video watermarking scheme based on Laplacian pyramid, SVD, and DWT with improved robustness towards geometric attacks via SURF," Multimed. Tools Appl., 2020. <u>https://doi.org/10.1007/s11042-020-09258-x</u>
- [12] M. M. Laftah, "3D Model Watermarking based on Wavelet Transform", Iraqi Journal of Science, vol. 62, no. 12, pp. 4999–5007, Dec. 2021. <u>https://doi.org/10.24996/ijs.2021.62.</u> <u>12.36</u>
- [13] J. Panyavaraporn, "DWT/DCT-based Invisible Digital Watermarking Scheme for Video Stream," 2018 10th Int. Conf. Knowl. Smart Technol., pp. 154–157. <u>https://doi.org/ 10.1109/KST.2018.8426150</u>
- [14] K. Meenakshi, K. Swaraja, and P. Kora, A robust DCT-SVD based video watermarking using zigzag scanning, vol. 900. Springer Singapore, 2019. <u>https://doi.org/10.1007/978-981-13-3600-3\_45</u>
- [15] A. F. Mahdi and M. T. Abd Al-Had, "Video Authentication By Visible Watermarking," Journal of Al-Ma'moon College., vol. 2017, no. 30, pp. 255-279, 2017. <u>https://doi.org/ 10.36458/1253-000-030-014</u>
- [16] K. J. Giri, S. M. K. Quadri, R. Bashir, and J. I. Bhat, "DWT based color image watermarking: a review," Multimed. Tools Appl., vol. 79, no. 43–44, pp. 32881–32895, 2020. <u>https://doi.org/10.1007/s11042-020-09716-6</u>

- [17] T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD," Futur. Gener. Comput. Syst., vol. 101, pp. 1223–1246, 2019. <u>https://doi.org/10.1016/j.future.2019.07.064</u>
- [18] K. Fares, A. Khaldi, K. Redouane, and E. Salah, "DCT & DWT based watermarking scheme for medical information security," Biomed. Signal Process. Control, vol. 66, no. December 2020, p. 102403, 2021. https://doi.org/10.1016/j.bspc.2020.102403
- [19] X. Liu, D. Xiao, W. Huang, and C. Liu, "Quantum Block Image Encryption Based on Arnold Transform and Sine Chaotification Model," IEEE Access, vol. 7, pp. 57188–57199, 2019. <u>https://doi.org/10.1109/ACCESS.2019.2914184</u>
- [20] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," Nonlinear Dyn., vol. 87, no. 1, pp. 127–133, 2017. <u>https://doi.org/10.1007/s11071-016-3030-8</u>
- [21] V. G and R. M, "A Survey on Image Encryption using Chaos-based Techniques," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 1, pp. 379–384, 2021. <u>https://doi.org/10.14569/ IJACSA.2021.0120145</u>
- [22] M. A. AlZain and O. S. Faragallah, "Efficient Chaotic Tent Map-based Image Cryptosystem," Int. J. Comput. Appl., vol. 167, no. 7, pp. 12–17, 2017. <u>https://doi.org/10.5120/ijca-2017914237</u>
- [23] M. R. Keyvanpour, N. Khanbani, and M. Boreiry, "A secure method in digital video watermarking with transform domain algorithms," Multimed. Tools Appl., vol. 80, no. 13, pp. 20449–20476, 2021. <u>https://doi.org/10.1007/s11042-021-10730-5</u>
- [24] R. Shoitan, M. M. Moussa, and S. M. Elshoura, "A robust video watermarking scheme based on Laplacianpyramid, SVD, and DWT with improved robustness towards geometric attacks via SURF," Multimed. Tools Appl, vol.79, no. 35-36, pp. 26837–26860, 2020. https://doi.org/10.1007/s11042-020-09258-x
- [25] I. A. Aljazaery, J. S. Qateef, A. H. M. Alaidi, and R. a. M. Al\_airaji, "Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN," International Journal of Interactive Mobile Technologies, vol. 16, no. 8, 2022. <u>https://doi.org/10.3991/ ijim.v16i08.30107</u>
- [26] R. M. Al\_airaji, I. A. Aljazaery, and S. K. Al\_dulaimi, "Generation of high dynamic range for enhancing the panorama environment," Bulletin of Electrical Engineering and Informatics, Article vol. 10, no. 1, pp. 138-147, 2021. <u>https://doi.org/10.11591/eei.v10i1.2362</u>
- [27] H. T. Salim, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 144-157, 2021. <u>https://doi.org/10.3991/ijim.v15i16.24557</u>
- [28] R. A. Azeez, M. K. Abdul-Hussein, and M. S. Mahdi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," Periodicals of Engineering Natural Sciences, vol. 10, no. 1, pp. 178-187, 2021. <u>https://doi.org/10.21533/pen.v10i1.2577</u>
- [29] H. T. Hazim, and N. Alseelawi, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT " vol. International Journal of Interactive Mobile Technologies (iJIM), 2021. <u>https://doi.org/10.3991/ijoe.v18i03.28011</u>
- [30] I. A. Aljazaery, and M. R. Aziz, "Combination of hiding and encryption for data security," International Journal of Interactive Mobile Technologies, Article vol. 14, no. 9, pp. 34-47, 2020. <u>https://doi.org/10.3991/ijim.v14i09.14173</u>
- [31] P. Ayubi, M. Jafari Barani, M. Yousefi Valandar, B. Yosefnezhad Irani, and R. Sedagheh Maskan Sadigh, A new chaotic complex map for robust video watermarking, vol. 54, no. 2. Springer Netherlands, 2021. <u>https://doi.org/10.1007/s10462-020-09877-8</u>

- [32] N. A. Ali, "Data Hiding in 3D Model Based on Surface Properties", Iraqi Journal of Science, vol. 64, no. 2, pp. 973–983, Feb. 2023. <u>https://doi.org/10.24996/ijs.2023.64.2.39</u>
- [33] N. Alsalam Ali, A. M. S. Rahma, and S. H. Shaker, "3D Polygon Mesh Encryption Based on 3D Lorenz Chaotic Map", Int. J. Interact. Mob. Technol., vol. 15, no. 15, pp. pp. 103– 114, Aug. 2021. <u>https://doi.org/10.3991/ijim.v15i15.24177</u>
- [34] M. Majeed Laftah, "Image Denoising Using Multiwavelet Transform with Different Filters and Rules", Int. J. Interact. Mob. Technol., vol. 15, no. 15, pp. pp. 140–151, Aug. 2021. <u>https://doi.org/10.3991/ijim.v15i15.24183</u>

# 8 Authors

**Muna Majeed Laftah** is presently Asst. Prof in Baghdad University/ College education for women/ Computer Science department. She received his B.Sc. degree in computer science in 1995 from the Al Technology University in Baghdad, Iraq. Her M.Sc. degree in computer science focuses on multimedia security from the Iraqi Commission for Computers and Informatics /Iraq in 2003. Her Ph.D. degree in computer science from Al technology University in Baghdad, Iraq/2017. Her current research interests include 3D security, encryption of multimedia (email: <u>mu-</u><u>na.majeed@coeduw.uobaghdad.edu.iq</u>).

**Iman I. Hamid** is a member of the college of education for women, computer science department, University of Baghdad, Iraq. She received his B.Sc. degree in Computer Science in 2000 from Mustansiriyah University in Baghdad, Iraq. Her M.Sc. degree in Computer Science from Iraqi Commission for Computers and Informatics in Baghdad, Iraq. She can be contacted at (email: <u>iman.hamid@coeduw.uobaghdad.edu.iq</u>).

Nashwan Alsalam Ali is a member of the college of education for women, computer science department, University of Baghdad, Iraq. He received his B.Sc. degree in computer Science in 2003 from Technology University in Baghdad, Iraq. His M.Sc. degree in Computer Science focuses on Multimedia Security from Iraqi Commission for Computers and Informatics in Baghdad, Iraq. His Ph.D. in Computer Science, Technology University in Baghdad, Iraq. He can be contacted at (email: nashwan\_alsalam60@coeduw.uobaghdad.edu.iq).

Article submitted 2023-01-12. Resubmitted 2023-02-28. Final acceptance 2023-03-04. Final version published as submitted by the authors.