ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 1, January 2022, pp.178-187

Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique

Raghad Abdulaali Azeez[1], Mohammad K. Abdul-Hussein[2], Mohammed Salih Mahdi[3], Haider TH. Salim ALRikabi[4]
[1] Computer Unit, Collage of Education for Human Science-ibn rushed, University of Baghdad, Baghdad, Iraq
[2]Al-Ma'mon University College, Department of Communication Engineering Baghdad, Iraq
[3] BIT, Business Information College, University of Information Technology and Communications, Baghdad, Iraq
[4]Wasit University, Wasit, Iraq

ABSTRACT

Copyright is a tool for preventing anyone forged to copy an electronic work from another person and claim that electronic work is referred to him. Since the identity of the person is always determined by his name and biometrics, there is a concern to handle this information, to preserve the copyright. In this paper, a new idea for copyright technology is used to prove video copyright, by using blind watermarking technique, the ownership information is hidden inside video frames using linear congruential generator (LCG) for adapted the locations of vector features extracted from the name and biometric image of the owner instead of hidden the watermark in the Pseudo Noise sequences or any other feature extraction technique. When providing the watermarked vector, a statistical operation is used to increase randomization state for the amplifier factors of LCG function. LCG provides random positions where the owner's information is stored inside the video. The proposed method is not difficult to execute and can present an adaptable imperceptibility and robustness performance. The output results show the robustness of this approach based on the average PSNR of frames for the embedded in 50 frames is around 47.5 dB while the watermark remains undetectable. MSSIM values with range (0.83 to 0.99).

Keywords: First keyword, Second keyword, Third keyword, Fourth keyword, Fifth keyword

Corresponding Author:

Raghad Abdulaali Azeez
Computer Unit, Collage of Education for Human Science-ibn rushed
University of Baghdad
Baghdad, Iraq
raghad.azeez@ircoedu.uobaghdad.edu.iq

1. Introduction

Many experts have lately expressed interest in a wide range of topics, including cloud computing, artificial intelligence, Internet of Everything, biometric image cryptography, steganography and copyright protection [1-15]. It makes a big difference whether you upload your data or third-party data to the cloud. Whoever is the only creator of a work, such as the author of an image, is free from all other legal requirements. using cloud computing to store third-party images, you must consider copyright. The situation is harder if you store information in a public cloud and sharing among several clients. situation if does not only a private ring of kin and friends. One of the permitted restrictions of copyright rules is the making of copies for particular goals [16]. Digital technology is handled various processes like duplicated, spread, uploaded in the cloud, and made it efficient open area effectively. Information integrity and copyright protection have become demanding matters and need to be resolved due to the ease of digital media modification. Misuse the privacy, made copyright owners obtain many individual advantages by undermining their real privileges for them. Watermark is an unnoticeable pattern that is embedded in data such as images, sound, and videos for a distinct of reasons, containing broadcast, signatures, publication monitoring, and copyright control, watermark must have two characteristics [17].
Robustness means that watermarked is incapable to removed, and if there is any try to remove it, the watermark is destroyed.

Invisibility means that watermarked is not sensitive to anyone or especially for attacker's vision, taking into consideration the quality of the image must not degrade. Electronic watermark copied is increased with the demand for electronic copy work. It is advantageous in handy applications, but electronic thefts exploit these features of digital works to robbery the legitimate rights of copyright owners to grow personal benefits. Advanced watermarking innovation still has an opportunity to move away better away to confirm watermark data, robust and limit of computerized watermarking One of the instruments to force the one's copyright is the watermarking. Watermark has more applications rather than copyright protection, the watermark can be used in authentication, which means that the integrity of the content of the watermark, not removed, not modified, a watermark can be used in tamper detection and localization by preventing not only external penetrative from stealing information from computer screen, but also insider penetrative to achieve personal benefits [18-22]. In recent years, biometrics get extend popularity in the security and copyright protection field. When started dealing with biometrics, this will diminish the traditional security methods such as password and remember it or change it at the time, and it is easy to stole by the hacker. Two types of biometrics are existing, physiological, and behavioral for example (fingerprint, facial, ear, iris, retina, handwriting, Keystroke patterning, Signature.... etc.), all these characteristics are uniqueness in individual to do recognition, identification, and authentication process [23, 24]. In this paper, a new proposed technique is used to approve the copyright of video file by embedded identity information (name, date of creating video, and iris biometric image), inside the video itself to confirm the copyright protection for this video, using random walk function LCG for allocating host positions to the identity information.

2. Related work

A lot of researches are done in using images and still images of video in the scope of copyright or watermark and these are employed using spatial or frequency domain, one of these research is presented by Woo C.S [25]. In his PhD thesis, the needing of strong watermark for copyright protection by develop blind watermark detection with low computational cost, and use a combination of transforms by creating a geometrical environment for a blind watermark, he improves semi-fragile watermarks by using wavelet domain, Peak to Signal Noise Ratio (PSNR) is used to evaluate his work, the highest value of PSNR is 20.98, where Hassan N.F., et al in [26] proposed a technique to embed the watermark inside digital video which is considered number of frames, the idea is to exploit corners and edges whenever are found in the frame. They used Canny, Sobel, Kirsch, and Prewitt to detect edges, and Harris Corner algorithm to detect corners. LSB technique is used for embedding watermarked text, Peak to Signal Noise Ratio (PSNR) is used to evaluate deformation in frames and video, the highest PSNR value for edges is 69.1884 and for corners is 80.0443. Hasan H.R [27] applied discrete wavelet transform algorithm (DWT) for (embedded/extracted) Blind watermarked, by divided RGB (cover/watermark) into three components which are R, G, and B, such that, R component is embedded in RW, G component is embedded in GW and B component is embedded in BW, this method has PSNR average about 44 dB and NCC value about 0.99. Bahrushin A. P., et al. [28] describe schema to hide a blind reversible watermark in a large data image using Even-Odd Modulation technique(EOM), this schema can embed "3145728 bits" watermark into the total volume of image 512×512 to achieve PSNR around 72 dB, and Mean Structural Similarity Index Measure (MSSIM) between embedded and recovered watermark is 1. A new crypto-watermarking system is suggested by Aparna P., et al. [29] face image was used with the medical image (X-RAY or else) and electronic health record (EHR) of the patient to send them from one hospital to another. This information is encrypted using AES encryption algorithm, the encrypted information is then compressed to improve the robustness of the system, PSNR ratio is achieved 44.6 dB, the capacity of embedded bits is 75,456, and NC equal 1. Non-blind watermark technique is proposed by Thanki R., et al. [30], instead of using pseudo-noise as watermark information, the technique is based on wavelet transform DCT and DWT using biometric image (signature), the process of embedding the watermark is done as follows: firstly, the host and biometric images are converted to different levels of the wavelet coefficients, secondly, the watermark biometric image is hidden in values of the modified wavelet of the host image corresponding to the values of the wavelet coefficients of a biometric image, the quality measure PSNR is achieved 52.00 DB. Mohammed S.J [31] presented video watermarking as a cover to hide iris biometrics in the audio part of the video instead of the images file of the video using frequency domain DCT and DWT, the chaotic sequence is used for two processes, first, to find locations in the video file to embed iris image watermark, second, the chaotic sequence is used to as a key to generate encrypted watermarking code and then embedded this code in audio multimedia of video file, to improve watermarking robustness.

3. Video watermark

Video watermarking is the procedure of hiding watermark in the frames of the video, or in the audio part of the video, the frames are considered as a sequence of video images. Video watermarking techniques are classified into Spatial domain, Frequency domain, and Format-specific, there are some advantages and disadvantages in using spatial or frequency domain, like in spatial domain, watermarking technique is fast, easy, and give high capacity, but it is not robust, in another hand, the frequency domain is robust but is slower than spatial technique. There are three ways for inserting watermark the video, first is, treat the video as a stream of still images, second is, utilize the additional temporal dimension, and third is, treat a video succession in data compression by specific video compression standards [32, 33]. Digital watermarking is characterized as blind or non-blind [34].

- Firstly, no information of the owner is utilized when recovering the embedded watermark on blind digital watermarking.
- However, secondly, additional sophisticated watermarking structure in non-blind digital watermarking, where few information of owners is utilized. The invisible watermarking is typically embedded as an impercipient. While, visible watermarking is typically purposely percipient.

4. Iris biometric pattern

Many applications of biometric characteristics are used security and copyright issues. The most popular are fingerprint and hand geometry, iris code, the shape of the ear, facial images, fingerprint, signature, voice characteristics, and DNA code. Each feature of these has its strengths and weaknesses, thus, no one biometric achieves the requirements of all applications. A biometric system may exploit in [35-39]

- Identification process, verifying the identity of user by matching the recorded biometric information to system database's biometric templates
- Authentication process, recognizing a user by for a matching, seeking the templates of all people in the database. Most of the above processes need prior operations in image processing to get the most accurate details for the original biometric image [40-45]. Iris biometric features are used to validate the owner of copyright. There are two reasons to select iris images [46, 47].

1- Automatic iris biometric recognition is possible by using mathematical models and physical techniques to prove the uniqueness of iris for each individual since each iris wavelength has various features of the iris within one Near-infrared ray (NIR) and visible wavelength (VW), these techniques sense the information from the iris by obtaining its texture and pigmentation that distinguishes one person from another.

2- Iris biometric serves the work is on watermark, since small storage for iris features is needed about 512 bytes per iris, and in addition to that, this biometric is not capable for modification or forgeries by the individual.

5. The proposed system

This paper focuses on using digital copyright using sill images of the host video to protect video from any attacks try to tamper on copyright; iris image biometric is used in creating the watermark as shown in the figure.

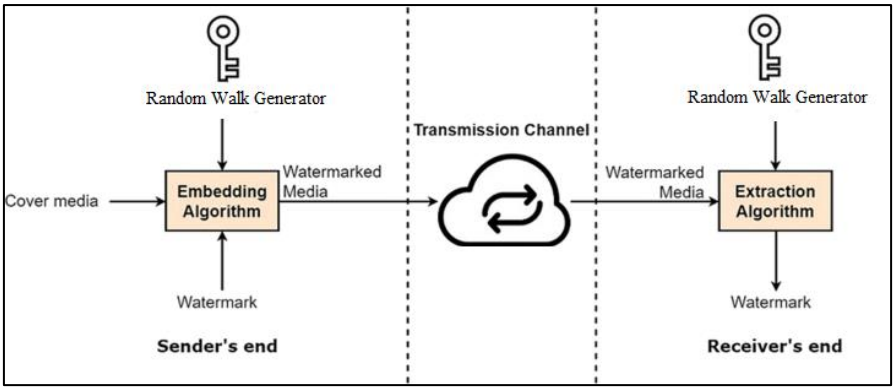

Figure 1. Scenario architecture of the proposed system

Figure 1 shows scenario architecture of the proposed system based on Watermarking over the Cloud. Sender transmit embedded watermark video on cloud provider based on random walk generator map. The receiver transmits the request for embedded watermark video to the cloud provider. The cloud provider transmits the requested embedded watermark video to the receiver. Now, a receiver can extract a watermark. The proposed system is passed through two phases:

Phase One: Generating the biometric watermarking vector and linear congruential generator:

In this part, watermarked vector-based exactly on iris image which is derived from MMU-Iris-Database [48] is explained, passing images of MMU_iris among set of operation like Gaussian_Blur filter, Canny_edge detector, and Hough Circle Transform with different Radius to extract the iris. The required owner information which is related to the owner (name and iris image) is determined to generate the watermark vector, statistical process is needed to achieve randomization assist in finding the factors of random walk generator as a linear congruential generator (LCG) for providing random position for watermarking. The following algorithm is describing the steps of the proposed watermarking vector and linear congruential generator. Cloud computing can be benefited in this concern [49].

Algorithm 1: Pproposed watermarking vector and random walk generator

Input: iris image, owner name and other information(optional)

Output: watermarking vector and random walk generator

Begin

Step$_1$: encode owner name and other information(optional) like date birth in ASCII Code in one-dimension vector which is called personal_info.

Step$_2$: implement Gaussian_Blur filter (7*7) on iris image.

Step$_3$: implement the Canny_edge detector on the output image of Step$_2$.

Step$_4$: extract pupil_ region by implementing Hough Circle Transform on output image of Step$_3$ With max_Radius=30 as an inner white circle and multiply with input iris image, and then subtract with 255.

Step$_5$: extract outer_ circle of iris by implementing Hough Circle Transform on output image of Step$_3$ With max_Radius=60 as an outer white circle and multiply with input iris image, and then subtract with 255.

Step$_6$: extract the region of interest (IRIS) by subtracting between the output image of Step$_4$ and the output image of Step$_5$ and store it as a one-dimension vector which is called personal_iris.

Step$_7$: compute median and mean for personal_iris and store as median_ personal_iris and mean_personal_iris.

Step$_8$: compute median and mean for personal_info and store as median_ personal_info and mean_personal_info of Step$_1$.

Step$_9$: Implement the following procedure for calculating linear congruential generator:

```
xa=int(round(median _personal_info))% width of iris image
seed_x = int(round(mean _personal_info))% width of iris image
ya=int(round(median _personal_iris))% height of iris image
seed_y = int(round(mean _personal_iris))% height of iris image
res=[]
for each c in range(length of (personal_info+ personal_iris )):
      res.append ([seed_x,seed_y])
      seed_x = (xa * seed_x + c) % width of iris image
      seed_y = (ya * seed_y + c) % height of iris image
```

Step$_{10}$: store the output result of Step$_9$ as random walk generator.

Step$_{11}$: combine personal_info and personal_iris as watermarking vector

End

Phase two: embed the watermark

After all stages from the previous phase are accomplished, watermarked vector and random walk generator (LCG equation) is created to be embedded in video frames that's mean the owner wants to insert copyright protection in the video file the steps of this phase is illustrated in Figure 2. Host position values are located by using random walk generator.

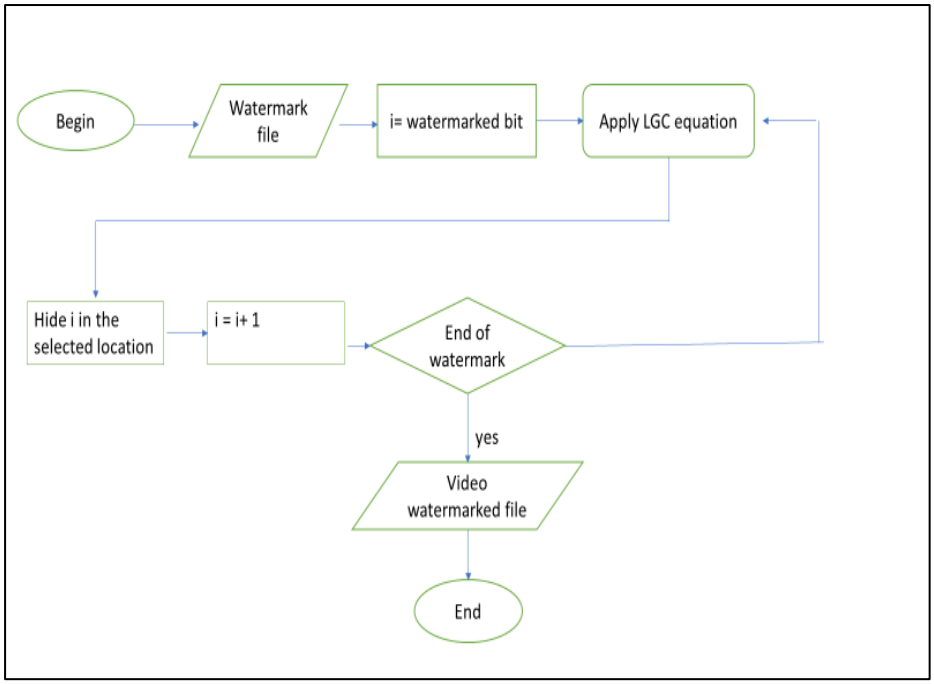

Figure 2. Diagram of Embedded the Watermark in Video File

Random Walk Generator is a mathematical process that describes randomly path that consists of a series of random steps on some mathematical area. Thus, to generate arbitrary series of values of locations. Arbitrary moves are utilized where these moves are of constant predetermined size. The procedure of randomness various according to the walking space. The linear congruential generator utilizing random walk according to the following equations as shown in the algorithm (1).

$$seed\_x = (xa * seed\_x + c) \% \text{ width of iris image} \quad \text{------ (1)}$$
$$seed\_y = (ya * seed\_y + c) \% \text{ height of iris image} \quad \text{------ (2)}$$

The parameters (xa and ya) are numbers that are selected so accurately based on mean and median of personal_iris, in order to overcome the computational load, one must restrict the range of the multiplier by using modular.
The following algorithm is the main process of the proposed system:

Algorithm 2: Embed Watermark in video
Input: video, watermarking vector, and random walk generator vector
Output: ***Embedded video***
Begin **Step$_1$**: convert video to frames. **Step$_2$**: convert watermarking vector in binary format **Step$_3$**: embed each 64 bit of watermarking vector for each frame in video frames based on located position random walk generator vector **End**

6. Results

Some practical results obtained with our proposed approach, for the testing format, 320x240 images from the MMU IRIS dataset as shown in Figure 3 and actual video sequences as shown in Figure 4 have been used. The watermark vector is indicated to a binary format as a combination of personal-info and personal iris.

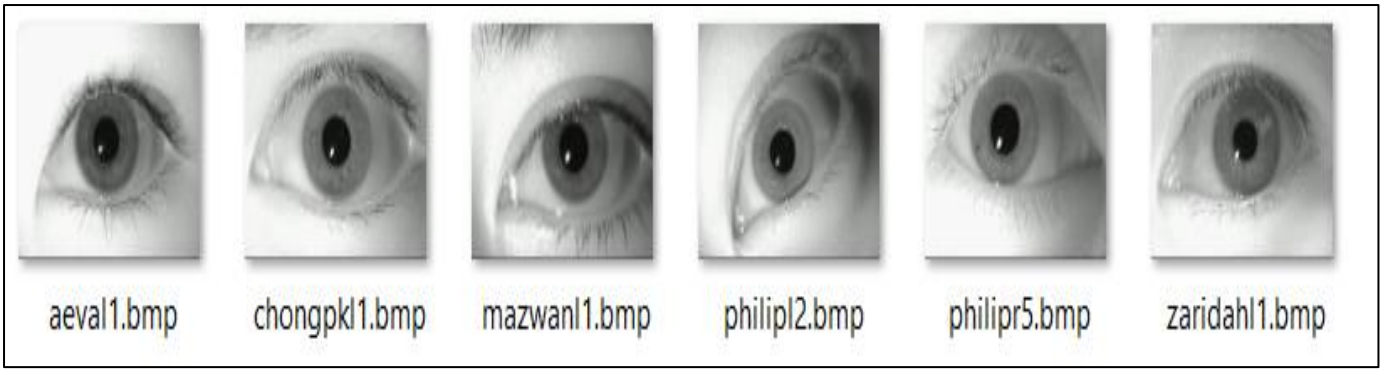

Figure 3. Sample of images from the MMU IRIS dataset

Figure 4. Sample of standard videos

Sample of Random Walk Generator is consisting of a series of random positions of pixels as shown in Figure 5 which is refers to the position of frame in video that will be embedding the watermark vector.

[109, 79], [259, 159], [270, 160], [212, 2], [175, 165], [229, 169], [144, 14], [310, 180], [177, 187], [135, 35], [274, 204], [24, 214], [115, 65], [297, 237], [20, 10], [314, 104], [309, 39], [75, 55], [22, 152], [220, 90], [119, 109], [109, 209] , [280, 150]

Figure 5. Sample of Random Walk Generator

Region of Iris that is taken from iris images among set of operation shown in Figure 6, like Gaussian_Blur filter, Canny edge detector and Hough Circle Transform with different Radius (30 ;60).

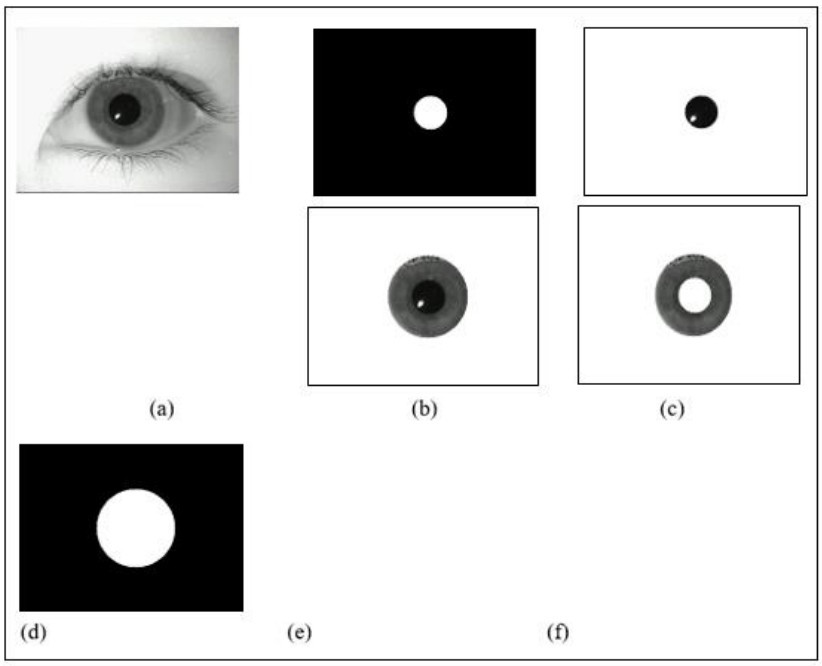

Figure 6. Region of segmented iris

PPSNR and MSSIM between the embedded and extracted copyright are mainly two criteria utilized to assess the experimental findings and estimate the performance of the proposed scenario. Table 1 clearly shows that the average PSNR of frames for the embedded in 50 frames is around 47.5 dB while the watermark remains undetectable. While, Table 2 presents MSSIM values with range (0.83 to 0.99).

Table 1. PSNR values for test video

No of Frame	PSNR
1	40.2
5	45.7
10	43.2
30	39.6
50	47.5

Table 2. MSSIM values for test video

No of Frames	MSSIM
1	0.83
5	0.92
10	0.88
30	0.93
50	0.99

7. Conclusion

The control for the sharing images actually sits not with the cloud computing service, but with the client who presents the expanded access. Each client is answerable for ensuring that the point copyrights and copyrights

are noticed. Watermark offers a trustworthy approach to the trouble of a user in cloud computing in electronic copyrights protection. This paper proposes a copyright system that uses high-density area of iris images using python 3.9 and google cloud firestore, which play an important role in determining copyright protection. Special information about the owner and iris images are passed through many operations to create permuted and confused watermarks. Within the proposed watermarked, the special information is working as an identity, while iris serves as an identification item. The essential contributions of the paper specify a significant novel move to the security concerns related to the multi_watermark problem since the special information of the owner included the watermark. Using Random Walk Generator, increasing the scrambling positions of pixels in the frame. Moreover, the obtained results give the proposed algorithm high performance with robustness in watermarking application, and especially the watermark can be difficultly extracted by an enemy. this will achieve protection to any video file, the average PSNR of frames for the embedded in 50 frames is around 47.5 dB while the watermark remains undetectable. MSSIM values with range (0.83 to 0.99).

References

[1] H. K. Tayyeh, M. S. Mahdi, and A. A. AL-Jumaili, "Novel steganography scheme using Arabic text features in Holy Quran," *Int. J. Electr. Comput. Eng,* vol. 9, no. 3, p. 1910, 2019.

[2] M. S. Mahdi and N. F. Hassan, "A proposed lossy image compression based on multiplication table," *Kurdistan Journal of Applied Research,* vol. 2, no. 3, pp. 98-102, 2017.

[3] M. S. Mahdi and N. F. Hassan, "Design of keystream Generator utilizing Firefly Algorithm," *Journal of Al-Qadisiyah for computer science mathematics,* vol. 10, no. 3, pp. Page 91-99, 2018.

[4] A. Kadhim and M. Salih, "Proposal of new keys generator for DES algorithms depending on multi techniques," *Engineering Technology Journal,* vol. 32, no. 1 Part (B) Scientific, 2014.

[5] M. Mahdi and N. Hassan, "A suggested super salsa stream cipher," *Iraqi Journal for Computers Informatics,* vol. 44, no. 2, pp. 5-10, 2018.

[6] H. 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.

[7] H. Ansaf, H. Najm, J. M. Atiyah, and O. A. Hassen, "Improved Approach for Identification of Real and Fake Smile using Chaos Theory and Principal Component Analysis," *Journal of Southwest Jiaotong University,* vol. 54, no. 5, 2019.

[8] H. Ansaf, S. Hussain, H. Najm, and O. Hassen, "Face Smile Detection and Cavernous Biometric Prediction using Perceptual User Interfaces (PUIs)," 2021.

[9] H. Najm, H. Hoomod, and R. Hassan, "Intelligent Internet of Everything (IOE) Data Collection for Health Care Monitor System," *International Journal of Advanced Science and Technology,* vol. 29, no. 4, pp. 2341-2350, 2020.

[10] H. Najm, H. K. Hoomod, and R. Hassan, "A proposed hybrid cryptography algorithm based on GOST and salsa (20)," *Periodicals of Engineering Natural Sciences,* vol. 8, no. 3, pp. 1829-1835, 2020.

[11] M. S. Mahdi, N. F. Hassan, and G. H. Abdul-Majeed, "An improved chacha algorithm for securing data on IoT devices," *SN Applied Sciences,* vol. 3, no. 4, pp. 1-9, 2021.

[12] M. Mahdi, "Proposed Secure Internet of Everything (IoE) in Health Care," 2018.

[13] M. S. Mahdi, Y. M. Abid, A. H. Omran, and G. Abdul-Majeed, "A Novel Aided diagnosis schema for covid 19 using convolution neural network," in *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1051, no. 1, p. 012007: IOP Publishing.

[14] A. Al-zubidi, R. K. Hasoun, and S. Hashim, "Mobile Application to Detect Covid-19 pandemic by using Classification Techniques: Proposed System," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 34-51, 2021.

[15] M. S. Mahdi, R. A. Azeez, and N. F. Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps," *Periodicals of Engineering Natural Sciences,* vol. 8, no. 4, pp. 2138-2145, 2020.

[16] M. MS, "Proposed block cipher algorithm with cloud computing based on keys generator," *MS Thesis, University of Technology, Iraq,* 2013.

[17] H. Najm, H. Hoomod, and R. Hassan, "A New WoT Cryptography Algorithm Based on GOST and Novel 5d Chaotic System," *iJIM,* vol. 15, no. 2, 2021.

[18] Z. Meng, T. Morizumi, S. Miyata, and H. Kinoshita, "Design scheme of copyright management system based on digital watermarking and blockchain," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, 2018, vol. 2, pp. 359-364: IEEE.

[19] H. Najm, "Data Authentication for Web of Things (WoT) by Using Modified Secure Hash Algorithm-3 (SHA-3) and Salsa20 Algorithm," *Turkish Journal of Computer Mathematics Education*, vol. 12, no. 10, pp. 2541-2551, 2021.

[20] D. Gugelmann, D. Sommer, V. Lenders, M. Happe, and L. Vanbever, "Screen watermarking for data theft investigation and attribution," in *2018 10th International Conference on Cyber Conflict (CyCon)*, 2018, pp. 391-408: IEEE.

[21] C.-S. Woo, "Digital image watermarking methods for copyright protection and authentication," Queensland University of Technology, 2007.

[22] I. A. Aljazaery, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Interactive Mobile Technologies (iJIM)*, 2021.

[23] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE access*, vol. 7, pp. 5994-6009, 2018.

[24] M. Al-dabag, H. S. ALRikabi, and R. Al-Nima, "Anticipating Atrial Fibrillation Signal Using Efficient Algorithm," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 17, no. 2, pp. 106-120, 2021.

[25] Y.-R. Lin, H.-Y. Huang, and W.-H. Hsu, "An embedded watermark technique in video for copyright protection," in *18th International Conference on Pattern Recognition (ICPR'06)*, 2006, vol. 4, pp. 795-798: IEEE.

[26] N. F. Hassan, "Proposed Video Watermarking Algorithm based on Edge or Corner Regions," *Engineering Technology Journal*, vol. 36, no. 1 Part B, 2018.

[27] H. R. Hasan, "Copyright protection for digital certificate using blind watermarking technique," *Kurdistan Journal of Applied Research*, vol. 3, no. 1, pp. 75-79, 2018.

[28] A. Bahrushin, G. Bahrushina, and R. Bazhenov, "A reversible image watermarking scheme based on a new modulation mode of DCT coefficients," in *Journal of Physics: Conference Series*, 2019, vol. 1399, no. 3, p. 033025: IOP Publishing.

[29] P. Aparna and P. V. V. Kishore, "A blind medical image watermarking for secure e-healthcare application using crypto-watermarking system," *Journal of Intelligent Systems*, vol. 29, no. 1, pp. 1558-1575, 2020.

[30] R. Thanki, V. V. Dwivedi, and K. Borisagar, "Robust watermarking technique using different wavelet decomposition levels for signature image protection," *Journal of Information Communication Technology*, vol. 16, no. 1, pp. 157-174, 2017.

[31] S. Mohammed, "Embedding biometric watermarking in video file based on chaotic principle," *technology*, vol. 5, p. 7.

[32] T. Jayamalar and V. Radha, "Survey on digital video watermarking techniques and attacks on watermarks," *International Journal of Engineering Science Technology*, vol. 2, no. 12, pp. 6963-6967, 2010.

[33] I. A. Aljazaery, S. K. Al_Dulaimi, abd H. T. Salim, "Generation of High Dynamic Range for Enhancing the Panorama Environment," *Bulletin of Electrical Engineering*, vol. 10, no. 1, 2021.

[34] Y.-S. Lee, Y.-H. Seo, and D.-W. Kim, "Blind image watermarking based on adaptive data spreading in n-level DWT subbands," *Security Communication Networks*, vol. 2019, 2019.

[35] M. A. Abdullah, S. S. Dlay, and W. L. Woo, "Securing iris images with a robust watermarking algorithm based on discrete cosine transform," in *International Conference on Computer Vision Theory and Applications*, 2015, vol. 2, pp. 108-114: Scitepress.

[36] J. Daugman, "How iris recognition works," in *The essential guide to image processing*: Elsevier, 2009, pp. 715-739.

[37] S. O. Olatinwo, O. Shoewu, and O. O. Omitola, "Iris recognition technology: implementation, application, and security consideration," *The Pacific Journal of Science Technology*, vol. 14, no. 2, pp. 228-33, 2013.

[38] S. N. Hasan, M. Gezer, R. A. Azeez, and S. Gülseçen, "Skin lesion segmentation by using deep learning techniques," in *2019 Medical Technologies Congress (TIPTEKNO)*, 2019, pp. 1-4: IEEE.

[39] D. Salman, R. Azeez, and A. Abdul-hossen, "BUILD CRYPTOGRAPHIC SYSTEM FROM MULTI-BIOMETRICS USING MEERKAT ALGORITHM," *Iraqi Journal for Computers Informatics*, vol. 45, no. 2, pp. 1-8, 2019.

[40] D. D. Salman, R. A. Azeez, and A. M. Hossen, "Key generation from multibiometric system using meerkat algorithm," *Engineering Technology Journal*, vol. 38, no. 3, pp. 115-127, 2020.

[41] H. Tauma, 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.

[42] D. Dahl, C. Atwood, and R. LaViolette, "A random-walk pseudorandom byte generator," *Applied Mathematical Modelling*, vol. 24, no. 10, pp. 771-778, 2000.

[43] M. Khalaf, H. Najm, A. A. Daleh, A. H. Munef, and G. Mojib, "Schema Matching Using Word-level Clustering for Integrating Universities' Courses," in *2020 2nd Al-Noor International Conference for Science and Technology (NICST)*, 2020, pp. 1-6: IEEE.

[44] H.-C. Tang, "Effective and efficient restriction on producing the multipliers for the multiple recursive random number generator," *Computers Mathematics with Applications*, vol. 47, no. 8-9, pp. 1309-1315, 2004.

[45] H. Najm, H. Ansaf, and O. A. Hassen, "An Effective Implementation of Face Recognition Using Deep Convolutional Network," *Journal of Southwest Jiaotong University*, vol. 54, no. 5, 2019.

[46] H.-C. Tang, "An analysis of linear congruential random number generators when multiplier restrictions exist," *European journal of operational research*, vol. 182, no. 2, pp. 820-828, 2007.

[47] N. F. Hassan, A. E. Ali, T. W. Aldeen, and A. Al-Adhami, "Video mosaic watermarking using plasma key," *Indonesian Journal of Electrical Engineering Computer Science*, vol. 22, no. 2, pp. 11-20, 2021.

[48] M. U. I. d. f. B. A. system, "MMU iris dataset," *https://www.kaggle.com/naureenmohammad/mmu-iris-dataset*,, 2020.

[49] Y. S. Mezaal, H. H. Madhi, T. Abd, and S. K. Khaleel, "Cloud computing investigation for cloud computer networks using cloudanalyst", vol.96, no.20, pp. 6937- 6947, 2018.