DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

Survey: Recent Techniques of Image Fragile Watermarking

Hala k. Hussein[1], Ra'ad A. Muhajjar[2], Bashar S Mahdi[3]
[1, 2]*Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq,*
[3]*Department of Computer Science, University of Technology, Baghdad, Iraq*
[1]*itpg.hala.khalid@uobasrah.edu.iq ,*[2]*raad.muhajjar@uobasrah.edu.iq,*
[3]*bashar.s.mahdi@uotechnology.edu.iq*

Abstract*—Ease of access to digital images and the many images editing programs available, like photoshop. All this makes the Issue of protecting images against modification becomes essential. Some images contain crucial information that can risk a patient's life, such as medical images and e-government images that relate to citizen information and state or ministry security. The watermark was one of the essential methods for this type of protection, especially the fragile watermark, which is very sensitive to any attack. Because of its other characteristics, it was one of the techniques that proved its efficiency in detecting tampering and the authenticity of images—also, watermarking focuses on protecting the image itself, not about protecting the secret message. A fragile watermark is a watermarking which inserts some information to cover an image to secure it .fragile watermarking could use in such a way and implement in spatial or frequency domain or in both so, making it a hybrid watermarking scheme. The Paper presented set of fragile watermark techniques used by the researchers with the performance metrics of an algorithm used in spatial and frequency domains, also showing how to use artificial intelligence with a watermarking technique to protect Document images from manipulation and forgery.*

Index Terms*— fragile watermark, spatial domain, frequncy domain*

I. INTRODUCTION

Nowadays, image protection is a critical concern. It covers a variety of topics such as information hiding, picture encryption, watermarking, and so on. All of them are distinct methods for securing digital images [1]. As a result, understanding how to prevent unauthorized copying, authentication, and integrity of data is important [2].

Due to the rising general demand for security, information hiding methods are continually changing and can be a suitable solution to these problems. Watermarking is a technique for embedding concealed information in digital material still developing [3]. The practice of embedding information on a picture so that text or logo images can be noticeable or not even seen without causing damage to the image is referred to as digital watermarking. Watermarking is a technique enabling proving the identity and authenticity of a digital image or signal owner. Signals such as video, images, or audio can be used [4]. An embedded watermark is detected using a statistical or similarity test or measuring a quantity particular to the watermark [5].

The different types of watermarking are as follows: robust, fragile, and semi-fragile, per the robustness, and classifiable according to perceptivity, watermarking comes in two:

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

visible and invisible, so depending on the application, users must decide which type of watermarking to apply. In cases where the most strong watermarking is required, robust watermarking can be used. As a result, if a sensitive and fragile system is used, they will be fragile or semi-fragile [6].

II. FRAGILE WATERMARKING

Fragile watermarking is a method for concealing confidential pieces of information in the host image. It is susceptible to changes in the image's contents. It's gained because it is perfect for authenticating content and image integrity investigation in scenarios when actual authentication is required. A modified image, for example, can lead to inaccurate diagnosis and treatment in the medical field. The fabricated image is introduced as proof of the legal preceding cause's misjudgment, i.e., the fake news image deceives the people. Fragile watermarking technologies are now required to determine the legitimacy of these critical conditions[7], [8].

III. FRAGILE WATERMARKING PROPERTIES

Below are some basic requirements for fragile watermarking techniques, as shown in *Fig. 1*:

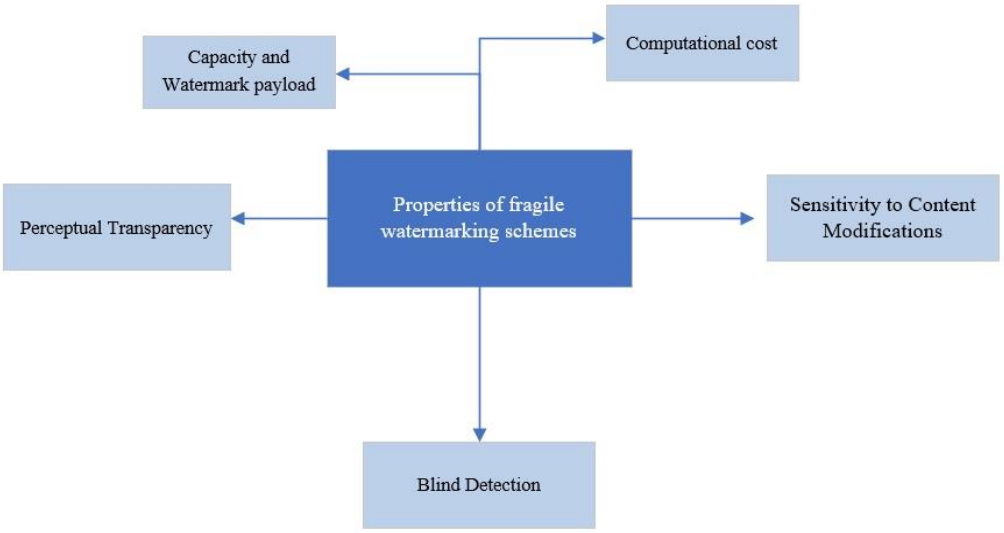

FIG.1. PROPERTIES OF FRAILGE WATERMAKING.

A. **The watermark's sensitivity**: An approach must be capable of determining whether or not the images have been modified with a high degree of certainty, even if the alteration is minimal. It is only achievable if a watermark of the images is responsive to every change in the contents [7], [8].

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

B. **Watermark payload and capacity**: It refers to the amount of information that can be stored in the digital medium that is being utilized, which varies based on the application[9].

C. **Cost of computation:** The cost of computing is usually expressed relating to embedding duration, watermark extraction time, tampered region localization time, and tampered region recovery time. The technique is more scalable because of its reduced computational cost [7], [8].

D. **Blind detection:** The fragile watermark can detect tampering even without a reference image [7], [8].

E. Perceptual transparency is the match between a watermarked image and its original counterpart. The image quality should not be degraded or affected in any way by the watermark [10].

IV. REVIEW FRAGILE WATERMARKING TECHNIQUES

Whether fragile, semi-fragile, or robust, all watermarking operations involve two procedures: embedding and extraction. This paper offers a summary set of the techniques of the embedding processes in the spatial and frequency domains.

A. Spatial domain

In the case of spatial embedding, the insertion is accomplished by altering the pixel's value. by using image pixels to conceal watermarking message bits and using Least Significant Bit (LSB) technology to replace the original image bit with one of the watermark bits [11].

J. Abd-Alhameed, and A. Ahmad [12] Suggested inserting fragile and robust watermarks were in method, each specified clearly. The images divide via three different channels Red Green Blue (RGB) and employ a green channel. To create a robust watermark, they used wavelet transformation. Each block from the green channel was separated into four blocks .then embedded into (low low frequencies) in frequency domain by using a phone number with its international code as the information data for robust watermarking. In the fragile watermarking process, apply a hash function to all RGB and consider the result as fragile watermark information, and use LSB in the embedding process.

D. Singh, S. S. and S. A. [13] Suggested utilizing three different methods to generate three authentication bits from each original image pixel known Authentication bit1, Authentication bit2 and Authentication bit3. To generate Authentication bit1 calculated the hamming distance of five Most Significant Bit (MSB) and created a pseudo-random random binary matrix. Then, the bitwise decimal sum was used to produce Authentication bit2 and to generate Authentication bit3 by a set of mathematical operations and bit Right Shift was used. Finally, these three authentication bits would be the watermark and then embedded into three Least Significant Bit (3LSB) corresponding pixels in the original image. The tamper localization problem can be solved using the provided method without impacting the visual quality.

A.Singh and M.K Dutta [14] The presented technique on medical images is divided into two sections: the first is Region of Interest (ROI), and the second is Region of Non-Interest (RONI). Because the ROI contains critical information, the initial step is to isolate ROI and RONI using pre-processing operations. Because it would affect the diagnosis if

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

tampered with it. The calculated average intensity value of each ROI generated the watermarked image, which was then embedded using the Least Significant Bit (LSB) approach in RONI. This approach is undetectable and sensitive to practically all attacks. It is also performed on CT scan images of the lungs.

In R. Munir [15] method produces a chaotic image that is dependent on the original value. Used a logistic map that makes actual values in the range of 0 to 1 to generate a chaotic image; convert it to integers and obtain binary bits. Then XOR with the watermarked image to encrypt. This watermark is XOR-ed between an original binary logo and a chaotic image, and it was embedded within the image by LSB.This scheme produced a high PSNR.

S.A Pinjari and N.N Patil [16] Worked on dividing the image into 3×3 blocks and used the concept of Local Binary Pattern (LBP) to display the neighborhood information for each block (LBP) to obtain the authentication data and create a fragile watermark embedded in Two Least Significant Bit (2LSB). LBP-based watermarking approaches have founded to have a relatively good tamper detection rate.

N.R.N Raj and R. Shreelekshmi [17] Suggest for adding security they used two fragile watermarks. In the beginning, they divided 8x8 blocks of the host image. Then used Message-Digest Five (MD5) to construct a 128-bit representation. Two Least Significant Bit (2LSB) represents the initial fragile watermark and embeds it in each block. The second technique is the same as the first, but it divides the image into 16*16 blocks. The Secure Hash Algorithm (SHA-256) function calculated the watermark; 256 bits are generated and stored in the cover image's LSB.

Rakhmawati et al. [18] Suggested created watermarks used crucial feature information from the original image in technique. procedure would aid in the phase of restoring damaged areas. To non-overlapping similar-sized blocks, they separated an image and worked on two bits: authentication and recovery in each, and then generated mapping of blocks using 1D transformation by determining the block's intensity average during insertion, replacing Three Least Significant Bit (3LSB) with watermarking bits. procedure results in an increase in Peak Signal-to-Noise Ratio (PSNR) and a perceived similarity between the original and watermarked image.

Wahid et al. [19] Worked on (MD5), a hash function technique that takes any input and returns a predetermined size, i.e., 128 bits. This technique would generate digital signatures as watermarks and then insert them into four Least Significant Bit (4LSB). For incorporating 128 bits, they'd require 32 pixels or 4 bits each pixel. There would be the same embedding in the extraction process but the opposite direction.

Ayu et al. [20] The proposed technique provided dual-layer fragile digital watermarking, in which two watermarks are embedded in medical images. They employed Advanced Encryption Standard (AES) to encrypt the Electronic Patient Record (EPR) for confidentiality and authenticity, then used Secure Hash Algorithm (SHA256) to validate Digital Imaging and Communication in Medicine (DICOM) tags' integrity after embedding them in 2LSB as the initial fragile watermark. Finally, they separated the image into non-overlapping blocks, assigned each one an id, then calculated the SHA256 for integrity and utilized it as a tamper detector.

E. Gul and G. Ozturk [21] Suggested using LSB to embed watermarking in the Spatial Domain. they created A watermark utilizing divide an image into four sub-blocks and processing the three sub-blocks through the SHA-256 hash algorithm .When extracting the watermark and comparing it against one generated by a hash function, see whether it was

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

tampered with and genuine. This condition reduces the authentication process's accuracy, especially for pixel-based attacks like salt and paper noise.

Shen et al. [22] The paper used Singular Value Decomposition (SVD) to create a fragile watermark that yields authentication information. They separated Non-overlapping blocks into two parts: upper and lower. It makes an authentication code via combining the information part of authentication from the bottom and top sections and embedding these codes in each block using 2 LSB. They could determine whether the block was tampered with or both after extracting the authentication information for each block and comparing it. The difficulty with this technique is that it can't handle image compression. Therefore it can't tell if an image was compressed using JPEG or Vector Quantization (VQ).

Molina-Garcia et al. [23] Suggested employing a color image to construct three recovery watermarks for the host image by dividing each color into 4×4 blocks, extracting 6 bits from each block, and then embedding the three watermarks for detection on the tampered region. They suggested using an inpainting process that aids in restoring the blocks that have been removed due to tampering coincidence problems. They also recommend using the technique 2LSB to keep image quality and apply hierarchal tamper detection to achieve high detection accuracy in extracting watermarks.

Sinhal et al. [24] paper used a color image and split it into 2×4 blocks non-overlapping by using a pseudo-random; they generated a random number between o and 1, then converted it to binary. This process results in a sequence of 6 bits that would be the fragile watermark. Following that, a series of operations will be applied, such as Least Significant Bit (LSB) and other procedures on each channel for RGB (Red, Green, Blue). Finally, in the extraction watermark, the block-wise classified as forgery or original according to neighbour blocks .in the recovery would use the six most significant bits. The problem with this schema is that it is block-wise, non-pixel-wise. That mean could detect which block was tampered not which pixel.

Gong et al. [25] Proposed a method demonstrates how to create fragile dual watermarks by combining diffusion and authentication watermarks. The secret key utilized with the cover image was selected using a collection of keys and a logistic map. It produced two random numbers using nonlinear transformations to make a diffusion watermark. For authentication watermark would be combined with another secret key and a cover picture. Finally, both would be embedded into the original image, resulting in an image with a watermark; however, because the extraction procedure is blind, they must reconstruct the authentication watermark and compare it.

E. Gul and S. Ozturk [26] Proposed used fragile watermarking pixel-wise authentication to detect and recover tamper location. They divided the image into four blocks, each split into two sub-blocks with sizes of 2×4 or 4×2. From these sub-blocks, they generated the recovery bit by using Six Most Significant Bit (MSB) of pixel and embedding it into 1LSB and 2LSB and by using two-pixel position bits to detect the tampered pixel. Instead of employing the Message-Digest Five (MD5) hash function, the primary technique used in the watermarking generating process is XOR.

Rinki et al. [27] Works on matrices multiplication and the three bits were replaced; in the process of embedding, the image is analyzed into the three colors: R, G, and B, where a matrix is created by selecting each determinant (6, 7, or 8) from each of these three colors and continues This continues until a 3×3 matrix is created, then the values of these pixels are converted to an 8-bit binary by padding bits, generating watermark image bits in matrix form. Finally, use the multiplication procedure to have the result matrix used in LSB in the

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

embedded processor to get the final watermarked image.The problem with this schema is that it's non-blind, requiring an original image.

Reyes-Reyes et al. [28] Have proposed a schema for RGB colour images, with the non-overlapping blocks separated from an image. They generate recovery also authentication watermarks from each block by applying Pseudocode to each channel. Red, green, and blue. They will have three watermarks that they can embed and provide more security in this stage. In the second stage, the bitwise exclusive OR (XOR) operation is done to each recovery watermark to generate a single bit for the block authentication process.

Su et al. [29] Proposed used the Sudoku game in hiding information which it was embedded fragile watermarking after generating it by Pseudo-Random Number Generator (PRNG). In-process extraction compares this one with that they embedded. They used a hidden information base two-layer .from the first layer extracts nine candidate pairs after that; from each pair, taking the block index and values index by Euclidian distance, they choose the final pair which carries the watermark.

B. Frequency domain

The embedding process in a frequency (transform) domain, also known as a transform domain. It is done using the transform coefficient. The image goes through sophisticated mathematical conversions to obtain the results. As a consequence, it appears more complex than the spatial domain.[30]

Cheng et al. [31] proposed fragile watermark was inserted into the host hologram. They performed embedding processes on the DCT domain. They quantize the value of a coefficient and the coefficient chosen for watermarking without creating higher perceptual distortion. As a result, the proposed technology could be a viable alternative for removing undesirable or illegal holograms from 3D displays for better efficiency.

Kunhu et al. [32] Use medical images, including sensitive information and information that must protect to maintain the image's integrity. They applied the notion of hyper watermark in their paper, applying both robust and fragile watermarks. The fragile watermark would use the hash function to identify tiny changes in images and embed them into Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) by dividing the image into Region of Interest (RIO) and RONI (region of non-interest). RIO was unable to include any information on watermark in the first embedded section, which could lead to incorrect diagnoses. It functioned by separating ROIN into three sub-blocks for watermark authentication, ownership, and information authentication. RIO authentication is verified using SHA 256, whereas RONI content authentication is verified using MD5.

H. and B. K. R. Joseph [33] suggested creating watermarking with a hybrid technique that included DCT and DWT characters. They embedded the concealed information in an image's DWT sub-bands. DCT was carried out in the DWT sub-bands that were defined. The watermark image was encoded and put in the original image using encryption technology. This method improves the image quality after watermarking and achieves imperceptibility and robustness.

Botta et al. [34] presented to improve the integrity of a 3D model specified in terms of a mesh of polygons by using the discrete Karhunen–Loève Transform (KLT), this method considered the vertex as Embedding Unit (EU) by used key generation. in the step of key generation KLT computed by a set of vectors that are driven from a secret image. KLT defines the hidden embedding space to insert the watermarking. One vertex at a time, utilizing the KLT basis and a genetic algorithm to change the vertex components in a

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

population of a hundred chromosomes, a Genetic Algorithm (GA) proceeds to the selection, crossover, and mutation steps. Also, every EU invokes the watermark generator module, which generates a watermark string. The watermark is embedded in the KLT coefficients of vertex data. This technique also includes a verifier, which aids in the process of locating tampered areas. This approach has a high sensitivity for any vertices that have been tampered with.

T. S. Nguyen [35] Proposed three algorithms using DWT, SVD, and DCT. They modify the coefficient of DCT to embed an authentication code, which generates by using a secret key and pseudo-random. For more quality, they split the image as 8x8 blocks that were non-overlapping. Then, they divide blocks of an image into four different coefficients to sub-bands using 1-level DWT. In order to avoid flaws, For the embedded authentication code, they extracted characteristics from the Low-Low sub-band using both SVD and DCT. In the step of watermarking extraction, as with the watermark embedding algorithm, the first three processes are all carried out similarly. Then check if the watermarked picture block has been tampered with by reconstructing the authentication code.

H. Barouqa and A. Al-Haj [36] Suggested inserting a watermark using discrete wavelet transformation (DWT), which separated host images into Low-Low, Low-High, High-Low, and High-High are non-overlapping sub-bands. This study is to solve the problem of copyright in black and white e-government documents. This approach gives us more process for whatever sub-band they choose. They used the complex eigenvalues of the Schur Decomposition at level two in a DWT to add a watermark. In this technique of watermarking, robustness it's required.

Botta et al. [37] Work on Neural Network Authenticity Checker (NeuNAC).Which uses two key technologies to integrate the watermark into the weights of such neural networks: the Karhunen-Loève Transform (KLT) and Gentic Algorithm (GA). The (KLT) pertains to the linear transformations category. They employ the hash function, which generates a length-fixed bit string. The (NeuNAC) is the Neural Networks Authenticity Checker algorithm. It adds the fragile watermark on a trained DNN's parameters without affecting the DNN's performance, impacting its to be able to execute at a level similar to before inserting a watermark. Parameter Unit (PU) generates the watermarking embedding and Table I provides a brief description of the techniques mentioned above.

TABLE I. LITERATURE REVIEW

Ref	Objective	Image type	Domain	Strategies	Performan e Metrics	Performance algorithm
12	The authentication and copyright	Mobile Phone Cameras Color image	Both transform and spatial Domain	DWT and LSB	PSNR, SSIM	PSNR > 45 dB. where SSIM more than 0.985 were produced by this algorithm
13	efficient pixel-wise fragile	Image of Gray	Spatial-domain	3LSB of original image	PSNR	PSNR value 40.8 dB and TDR value 98.21%
14	Even the tiniest alteration with the medical imaging can be detected	Lungs CT scan images	Spatial	LSB into RONI	PSNR,	Highly imperceptible and payload capacity more than35000 and PSNR it Almost 62.94 dB
15	Image integrity	Gray image	Spatial	Using Logistic Map to introduce chaotic image.	PSNR	PSNR are 51.1451 dB and 51.1446 dB.

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

Ref	Objective	Image type	Domain	Strategies	Performance Metrics	Performance algorithm
16	Enhance tamer detection rate	Gray image	Spatial	Local-Binary-Pattern (LBP)	PSNR,	This method show good tamper detection rate and PSNR > 43.53 dB
17	Tamper localization.	Color and Gray image	Spatial domain	Used 2 fragile watermark with SHA-256 algorithm	PSNR, SSIM, TPR, FPR	In method1.In terms of PSNR and SSIM, the average parametric values are51.14 and 0.9978 respectively. In method2 The average of PSNR and SSIM are44.147 and 0.9804.TPR Methods one and two both have a score of 100, while FPR is somewhat higher.
18	Improve-image quality	Gray image	Spatial	Tamper Detection and Recovery using 1D transformation	PSNR, BER	PSNR of This algorithm is 37.61dB and similar perceptual between original and watermarked image
19	Image integrity	Image with grey	Spatial	Hash MD5 and embedded them into 4LSB	PSNR	PNSR average is 66 db.
20	Ensuring the integrity of the medical image	Digital Imaging andCommuniatin in Medicine(DICOM)	Spatial	Dual-layer fragile technique	PSNR, MSE, SSIM	This techniques has PSNR values more than 44 dB, and SSIM values almost 1 ,MSE is 2.3
21	Image integrity	Image with grey	Spatial	SHA-256 with LSB modification.	PSNR	PSNR values exceed 57 dB
22	Enhances the ability of tamper recovery.	Image with grey	Spatial	Singular value decomposition (SVD)	PSNR, SSIM, FPR	The average PSNR of all images 47 db. and SSIM 0.983 and reduce the FPR down to 0.111%
23	Authentication and self-recovery for Color-Image	Image with grey	Spatial	Inpainting process	PSNR, SSIM and PSNR-HVS-M	PSNR, SSIM, and PSNR-HVS-M averaged 19.20 dB, 0.3958, and 15.11 dB, accordingly to 80 percent alteration reconstruction.
24	Effcient detection & recovery against block	RGB-images	Spatial	the pseudo random number generation algorithm	PSNR, SSIM, TR ,TDR	Regarding PSNR and SSIM, the average parametric results are 49.62 and 0.9986, respectively.,TR<=80% ,TDR=99.771%,
25	security of watermark	Image with grey	Spatial-domain	3D Arnold transformation	PSNR	PSNR is 44.17 dB and Sensitivity is almost 75.67%
26	Detects and recovers the manipulated areas.	Image with grey	Spatial	Process is XOR for watermarking generating	PSNR, SSIM	PSNR > 38 dB, SSIM > 0.92 which is higher in n the watermarked images.
27	Enhance the conventional LSB technique	RGB-images	Spatial	The LSB approach is based on the multiplication of matrices.	PSNR, NCC	PSNR with more than 54 dB , NCC almost 0.99
28	Authentication and self-recovery	Colors images	Spatial	The framework is self-recovery from a high tampering rate(SR-HTR)	PSNR, SSIM and PSNR-HVS-M	PSNR, SSIM, and PSNR-HSV-M values for recovering alteration ratios between 10% to 90% were PSNR 12.72 dB, PSNR-HSV-M is 14.41 dB, and SSIM is 0.3516

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

Ref	Objective	Image type	Domain	Strategies	Performance Metrics	Performance algorithm
29	Increases security and makes the concealed watermark undetectable	Image with grey	Spatial	Hybrid-Sudoku	PSNR, SSIM, UQI ,TDR	The average PSNR is 47.42 dB, SSIM is 0.9988, UQI is 0.9666, and TDR is99.72%
31	Used as an effective filter for tampered holograms	3D display	Frequency (transform) domain	DCT of hologram	PSNR,	The suggested technique gives a high level. With a PSNR of 50.08 dB, perceptual transparency is achieved.
32	The ownership protection and content authentication	X-ray and MRI medical images	Frequency (transf rm) domain	Hash algorithms that combine DWT-DCT and SHA256-MD5	PSNR, SSIM and WSNR	PSNR between 44.32 to 61.90 SIMM between 0.9645 to 1 WSNR between 44.37 to 64.91
33	Improve the image quality and achieve imperceptibility and robustness	Gray-scale	Frequency (transform) domain	Hybrid technique DCT and DWT characters	PSNR, MSE	PSNR is 51.01 and MSE is 0.52
34	Integrity protection and authentication	Mesh of polygons	Frequency (transform) domain	3D model watermarking Genetic algorithm	RMSE -PSNR	Show high Sensitivity 93.82 also high PSNR>299db.RMSE 3.19*10-13
35	Ensure that digital images are integrity.	Gray-scale	Frequency (transform) domain	DWT-SVD-DCT techniques	PSNR, NCC	PSNR greater than 84 dB also (NCC) greater than 0.99
36	Copyright	black and white e-governmet documents	Frequency (transform) domain	The Discrete Wavelets Transform and Schur Decomposition	NC	NC almost 0.8
37	Sophisticated for DNNs for use in safety-critical systems, including (semi) self-driving automobile systems	—	Frequency (transform) domain	NeuNAC (Neural Network Authenticity Checker) and Karhunen-Loève Transform (KLT)	PSNR, MSE, SSIM	The average PSNR is better than 181 dB, indicating good network performance.

V. CONCLUSIONS

In this research, twenty-five techniques used in the fragile watermark were presented in various fields and for color or gray images and in different application such as three dimansion or medical images.

In addition, participants discussed how strategies, objectives, performance metrics, and performance algorithms. PSNR has a high percentage of methods generated by artificial intelligence. The watermark increase in the PSNR measurement reached approximately in Neural Network Authenticity Checker, more than 181 dB. Also noticed that the watermark is embedded in the frequency domains for additional authentication. Still, if focus on the sensitivity and fragility of the watermark, it is therefore done embedded in a spatial domain.

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

REFERENCES

[1] I. Q. Abduljaleel, "Using IWT and LSB Method to Hide Encrypted image in Color image," *J. Basrah Res.*, pp. 1–16, 2016.

[2] C. Gu and X. Cao, "Research on information hiding technology," *2012 2nd Int. Conf. Consum. Electron. Commun. Networks, CECNet 2012 - Proc.*, pp. 2035–2037, 2012, doi: 10.1109/CECNet.2012.6201610.

[3] A. H. Khaleel and I. Q. Abduljaleel, "Secure image hiding in speech signal by steganography-mining and encryption," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1692–1703, 2021, doi: 10.11591/ijeecs.v21.i3.pp1692-1703.

[4] G. Kaur and K. Kaur, "Digital Watermarking and Other Data Hiding Techniques," *Int. J. Innov. Technol. …*, no. 5, pp. 181–183, 2013.

[5] A. I. Abdul-sada, "Hiding Data Using LSB-3," *J.Basrah Res.*, vol. 33, no. 4, 2007.

[6] P. Pal, H. V. Singh, and S. K. Verma, "Study on Watermarking Techniques in Digital Images," *Proc. 2nd Int. Conf. Trends Electron. Informatics, ICOEI 2018*, vol. 1, no. Icoei, pp. 372–376, 2018, doi: 10.1109/ICOEI.2018.8553743.

[7] K. Sreenivas and V. Kamkshi Prasad, "Fragile watermarking schemes for image authentication: a survey," *Int. J. Mach. Learn. Cybern.*, vol. 9, no. 7, pp. 1193–1218, 2018, doi: 10.1007/s13042-017-0641-4.

[8] N. R. N. Raj and R. Shreelekshmi, "A survey on fragile watermarking based image authentication schemes," *Multimed. Tools Appl.*, vol. 80, no. 13, pp. 19307–19333, 2021, doi: 10.1007/s11042-021-10664-y.

[9] H. M. Abdul-Nabi, Z. B. Dahoos, and M. M. Khudhair, "Enforcement of Color Image Copyright Using the Frequency Domain," *J. Basrah Res.*, vol. 35, no. 1, 2009, [Online]. Available: http://www.docudesk.com.

[10] H. A. Younis, "Robust Image Watermarking in the Wavelet Domain," *J. Kufa Math. Comput. Undefined*, vol. 1, no. 2, pp. 23–34, 2010, Accessed: Apr. 19, 2022. [Online]. Available: https://www.iasj.net/iasj/download/ccaf7fdc479182d2.

[11] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: A review of current research directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.

[12] T. Jassim, R. Abd-Alhameed, and H. Al-Ahmad, "New robust and fragile watermarking scheme for colour images captured by mobile phone cameras," *Proc. - UKSim 15th Int. Conf. Comput. Model. Simulation, UKSim 2013*, pp. 465–469, 2013, doi: 10.1109/UKSim.2013.83.

[13] S. S. and S. A. D. Singh, "Self-embedding Pixel Wise Fragile Watermarking Scheme for Image Authentication," *Commun. Comput. Inf. Sci.*, vol. 276 CCIS, no. January, 2013, doi: 10.1007/978-3-642-37463-0.

[14] A. Singh and M. K. Dutta, "A blind & fragile watermarking scheme for tamper detection of medical images preserving ROI," *2014 Int. Conf. Med. Imaging, m-Health Emerg. Commun. Syst. MedCom 2014*, pp. 230–234, 2014, doi: 10.1109/MedCom.2014.7006009.

[15] R. Munir, "A chaos-based fragile watermarking method in spatial domain for image authentication," *2015 Int. Semin. Intell. Technol. Its Appl. ISITIA 2015 - Proceeding*, pp. 227–231, 2015, doi: 10.1109/ISITIA.2015.7219983.

[16] S. A. Pinjari and N. N. Patil, "A pixel based fragile watermarking technique using LBP (Local Binary Pattern)," *Proc. - Int. Conf. Glob. Trends Signal Process. Inf. Comput. Commun. ICGTSPICC 2016*, pp. 194–196, 2017, doi: 10.1109/ICGTSPICC.2016.7955296.

[17] N. R. N. Raj and R. Shreelekshmi, "Blockwise Fragile Watermarking Schemes for Tamper Localization in Digital Images," *2018 Int. CET Conf. Control. Commun. Comput. IC4 2018*, pp. 441–446, 2018, doi: 10.1109/CETIC4.2018.8530950.

[18] L. Rakhmawati, Wirawan, and Suwadi, "Image Fragile Watermarking with Two Authentication Components for Tamper Detection and Recovery," *2018 Int. Conf. Intell. Auton. Syst. ICoIAS 2018*, pp. 35–38, 2018, doi: 10.1109/ICoIAS.2018.8494080.

[19] M. Wahid, N. Ahmad, M. H. Zafar, and S. Khan, "On combining MD5 for image authentication using LSB substitution in selected pixels," *2018 Int. Conf. Eng. Emerg. Technol. ICEET 2018*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/ICEET1.2018.8338621.

[20] M. A. Ayu, T. Mantoro, and I. M. A. Priyatna, "Advanced watermarking technique to improve medical images' security," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 5, pp. 2684–2696, 2019, doi: 10.12928/TELKOMNIKA.v17i5.13292.

[21] E. Gul and S. Ozturk, "A novel hash function based fragile watermarking method for image integrity," *Multimed. Tools Appl.*, vol. 78, no. 13, pp. 17701–17718, 2019, doi: 10.1007/s11042-018-7084-0.

[22] J. J. Shen, C. F. Lee, F. W. Hsu, and S. Agrawal, "A self-embedding fragile image authentication based on singular value decomposition," *Multimed. Tools Appl.*, 2020, doi: 10.1007/s11042-020-09254-1.

[23] J. Molina-Garcia, B. P. Garcia-Salgado, V. Ponomaryov, R. Reyes-Reyes, S. Sadovnychiy, and C. Cruz-Ramos, "An effective fragile watermarking scheme for color image tampering detection and self-recovery," *Signal Process. Image Commun.*, vol. 81, no. July 2019, p. 115725, 2020, doi: 10.1016/j.image.2019.115725.

[24] R. Sinhal, I. A. Ansari, and C. W. Ahn, "Blind Image Watermarking for Localization and Restoration of

Received 29/April/2022; Accepted 25/May/2022

ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.2.12

Color Images," *IEEE Access*, vol. 8, pp. 200157–200169, 2020, doi: 10.1109/ACCESS.2020.3035428.

[25] X. Gong, L. Chen, F. Yu, X. Zhao, and S. Wang, "A secure image authentication scheme based on dual fragile watermark," *Multimed. Tools Appl.*, vol. 79, no. 25–26, pp. 18071–18088, 2020, doi: 10.1007/s11042-019-08594-x.

[26] E. Gul and S. Ozturk, "A novel pixel - wise authentication - based self - embedding fragile watermarking method," *Multimed. Syst.*, no. 0123456789, 2021.

[27] K. Rinki, P. Verma, and R. K. Singh, "A novel matrix multiplication based LSB substitution mechanism for data security and authentication," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2021, doi: 10.1016/j.jksuci.2021.01.013.

[28] R. Reyes-Reyes, C. Cruz-Ramos, V. Ponomaryov, B. P. Garcia-Salgado, and J. Molina-Garcia, "Color image self-recovery and tampering detection scheme based on fragile watermarking with high recovery capability," *Appl. Sci.*, vol. 11, no. 7, 2021, doi: 10.3390/app11073187.

[29] G. D. Su, C. C. Chang, and C. C. Chen, "A hybrid-Sudoku based fragile watermarking scheme for image tampering detection," *Multimed. Tools Appl.*, vol. 80, no. 8, pp. 12881–12903, 2021, doi: 10.1007/s11042-020-10451-1.

[30] S. Lyatsky, "Digital Watermarking Techniques In Image Processing," The Catholic University of America, 2018.

[31] C. J. Cheng, W. J. Hwang, H. Y. Zeng, and Y. C. Lin, "A fragile watermarking algorithm for hologram authentication," *IEEE/OSA J. Disp. Technol.*, vol. 10, no. 4, pp. 263–271, 2014, doi: 10.1109/JDT.2013.2295619.

[32] A. Kunhu, H. Al-Ahmad, and F. Taher, "Medical images protection and authentication using hybrid DWT-DCT and SHA256-MD5 hash functions," *ICECS 2017 - 24th IEEE Int. Conf. Electron. Circuits Syst.*, vol. 2018-Janua, pp. 397–400, 2018, doi: 10.1109/ICECS.2017.8292084.

[33] H. and B. K. R. Joseph, "Image Security Enhancement using DCT & DWT Watermarking Technique," *IEEE*, pp. 940–945, 2020.

[34] M. Botta, D. Cavagnino, M. Gribaudo, and P. Piazzolla, "Fragile watermarking of 3D models in a transformed domain," *Appl. Sci.*, vol. 10, no. 9, 2020, doi: 10.3390/app10093244.

[35] T. S. Nguyen, "Fragile watermarking for image authentication based on DWT-SVD-DCT techniques," *Multimed. Tools Appl.*, vol. 80, no. 16, pp. 25107–25119, 2021, doi: 10.1007/s11042-021-10879-z.

[36] H. Barouqa and A. Al-Haj, "Watermarking E-Government Document Images Using the Discrete Wavelets Transform and Schur Decomposition," *2021 7th Int. Conf. Inf. Manag. ICIM 2021*, pp. 102–106, 2021, doi: 10.1109/ICIM52229.2021.9417146.

[37] M. Botta, D. Cavagnino, and R. Esposito, "NeuNAC: A novel fragile watermarking algorithm for integrity protection of neural networks," *Inf. Sci. (Ny).*, vol. 576, pp. 228–241, 2021, doi: 10.1016/j.ins.2021.06.073.

Received 29/April/2022; Accepted 25/May/2022
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*