Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.016382
Article

Tech Science Press

Secure Image Authentication Using Watermarking and Blockchain

Alsehli Abrar[1], Wadood Abdul[1,*] and Sanaa Ghouzali[2]

[1]Department of Computer Engineering, College of Computer and Information Sciences King Saud University 11543 Riyadh, Kingdom of Saudi Arabia
[2]Information Technology Department, College of Computer and Information Sciences
King Saud University, 11451 Riyadh, Kingdom of Saudi Arabia
*Corresponding Author: Wadood Abdul. Email: aabdulwaheed@ksu.edu.sa

Received: 31 December 2020; Accepted: 13 February 2021

Abstract: Image authentication is an important field that employs many different approaches and has several significant applications. In the proposed approach, we used a combination of two techniques to achieve authentication. Image watermarking is one of the techniques that has been used in many studies but the authentication field still needs to be studied. Blockchain technology is a relatively new technology that has significant research potential related to image authentication. The watermark is embedded into the third-level discrete wavelet transform (DWT) in the middle frequency regions to achieve security and imperceptibility goals. Peak signal-to-noise ratio PSNR, structural similarity matrix (SSIM), normalized correlation coefficient (NCC), and bit error rate (BER) are used to measure the performance of image watermarking. We used blockchain technology to avoid involving a trusted third party for authentication. Secure Hash Algorithm 256 (SHA-256) is applied on the watermark to save it into the blockchain. The watermark is encrypted using Advanced Encryption Standard (AES) and embedded into the image. The proposed method is tested on the USP SICI database and the MedPix medical image database. Ethereum blockchain is used to provide security, anonymity, and integrity of data with no third-party intervention. The proposed solution demonstrates enhanced security for image authentication compared with the state-of-the-art.

Keywords: Authentication; watermarking; DWT; encryption; security; hash; blockchain

1 Introduction

The importance of image authentication has emerged in lots of areas: martial images, images for proof in court, medical images, and several other research areas [1–3]. When dealing with these images and other types of images, there is a need for a security and authentication layer to avoid incorrect judgments. Digital image processing tools are widely available and easy to use, allowing easy access, manipulation, and reuse. These days, unauthorized copies of images could be easily made to manipulate images for financial or human life losses [4]. Authenticating an image is the operation of making sure that the person who provided the image is the same person with appropriate rights to the image. Image authentication has become a more important issue since the revolution of social media and the Internet. Given the important requirement for securing sensitive information that could threaten security, we need to identify and distinguish between real and fake images. In this work, we used two techniques to authenticate images; watermarking and blockchain. Watermarking is the process of inserting secret information into the digital image. The main elements of watermarking are watermark embedding and watermark extraction. The embedding process is used to add the watermark into the cover image; on the other hand, watermark extraction extracts the watermark from the image. The key is used during the watermarking process for securing the watermark embedding and extraction procedures. Blockchain is a distributed ledger technology that saves information to make sure that it will remain the same and not be changed by anyone. It also executes and shares all the digital events with the involved users [5]. The use of the blockchain is to accomplish authentication without the involvement of a trusted third party for the secrecy of the watermark so is not be exposed to anyone expect the involved parties. Our work has many benefits in the image authentication field. Many advantages have been achieved compared to previous works and the proposed work contributes the following to the state of the art. The proposed work was implemented with high imperceptibility and security. The encrypted watermark is embedded in the third level wavelet coefficients. The watermark is hashed and added to the blockchain to improve security.

The rest of the paper is organized as follows. Section 2 presents the related works followed by Section 3 that presents the secure watermarking approach. Experimental results are presented in Section 4 followed by the comparison with state-of-the-art methods in Section 5. The work is concluded in Section 6.

2 Related Works

In recent times, blockchain technology has gained lots of attention since it has been introduced in 2008 by Nakamoto. In Crosby et al. [6], descriptive literature on the blockchain has been introduced for the first time. The discussion is about the Bitcoin system and there is no real focus on blockchain technology. Blockchain is used in many industries, finance, medical, agriculture, smart city, internet of things, genetic engineering, energy industry, automobile insurance industry, cloud computing, cloud storage, and others. Hou [7] has introduced an E-government application of blockchain in China. Lim et al. [8] set up MyData for personal data management which was authorized by the Finnish government. A blockchain- cross-domain authentication model named BlockCAM, the cross-domain authentication protocol, has also been proposed in [9]. Liu et al. [10] introduced a combination of strong Physical Unclonable Functions (PUFs)-based authentication protocol and blockchain with Peer to Peer (P2P) distributed storage script.

A method for medical records is controlled and secured using blockchain based on a genetic algorithm and DWT is proposed in [11]. Blockchain technology has been used to provide a privacy consciousness authentication framework for a multi-server environment which was introduced by Xiong et al. [12]. Puthal et al. [13] presented a new consensus algorithm called proof of authentication for scalable blockchain. A personal data management approach that concentrates on privacy using blockchain has been produced by Zyskind et al. [14]. To accomplish fast authentication for vehicles and cooperative participation between vehicular networks, a distributed trust access authentication system is introduced relying on a blockchain network and edge computing [15]. A semi-fragile watermarking framework to increase the invisibility and manipulation recovery performance under JPEG compression is done by Chen et al. [16].

A new blind color image watermarking technique in the spatial domain was proposed by Su et al. [17]. The technique was used to get the highest eigenvalue of Schur decomposition. This eigenvalue is used when embedding and extracting the watermark. The semi-fragile watermarking method that relies on a rotation vector for content authentication purposes was introduced by Fu et al. [18]. Robust image watermarking in the Lifting Wavelet Transform (LWT) domain using more than one sub-band was proposed by Islam et al. [19]. This scheme embeds a binary watermark in the LWT sub-bands. During the extraction phase, Support Vector Machine (SVM) was used to increase the robustness. Image authentication is a field that has several methods and implementations. Combining watermarking and blockchain for image authentication is a relatively new field that still needs more research to achieve the objectives of security and imperceptibility.

3 Secure Watermarking using Hashing and Blockchain

The proposed method will introduce image authentication using watermarking and the Ethereum blockchain for gray-scale images in the frequency domains. The watermark embedding phase is shown and described in Fig. 1. First of all, the Discrete Wavelet Transform (DWT) in the third level is applied to the image that needs to be authenticated. The watermark is the image owner's ID hash number. Advanced Encryption Standard (AES) encryption with a secret key is used to encrypt the watermark which is then embedded into the middle frequency wavelet coefficients. The same watermark that is embedded into the image is hashed with SHA-256 and saved by the user depending on the user key into the blockchain. AES and SHA-256 are used together as an extra layer of security when embedding the watermark into the image and when saving the watermark into the blockchain. AES is used for encrypting the watermark before embedding into the image. SHA-256 is used to encrypt the watermark before saving it into the blockchain. SHA-256 is used as it is a one-way function and we do not want anyone to gain access to the watermark as a consequence of getting the AES key.

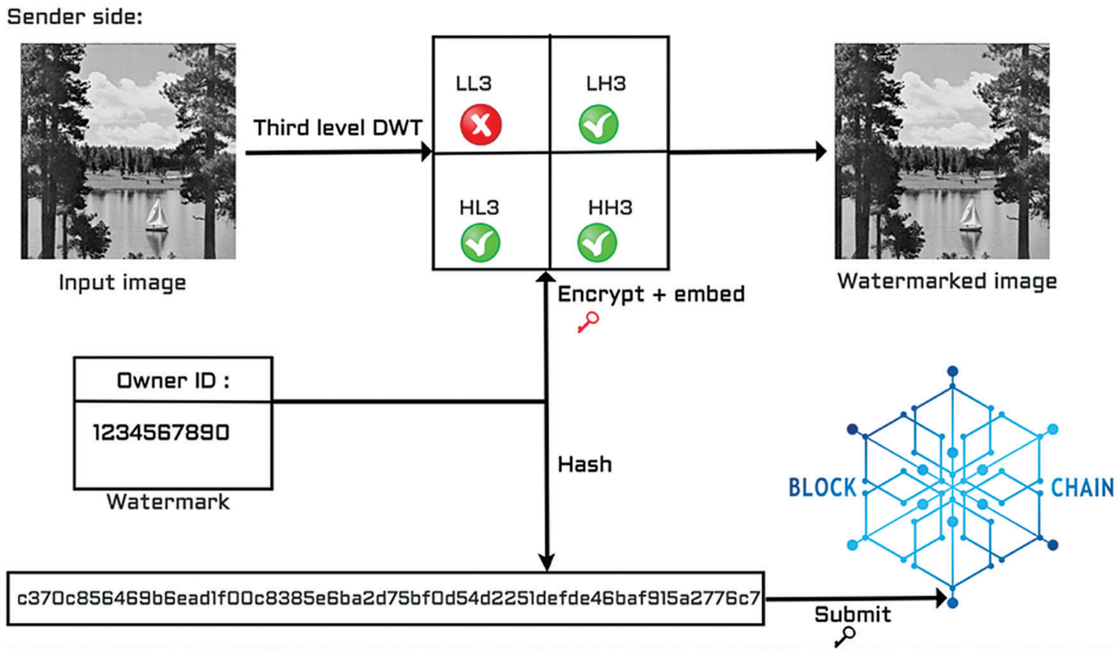

Figure 1: Proposed secure watermark embedding

The watermark extraction process is shown in Fig. 2. The extraction process is used when there is a need to check the authenticity of a received image. To authenticate a received image, the watermarked image and the encryption key are required for the watermark extraction from the image. We extract the encrypted watermark from the three middle frequency sub-bands of the image. Then the watermark is decrypted as shown in Fig. 2. Secure Hash Algorithm 256 (SHA-256) is applied onto the decrypted watermark. From the blockchain, we obtain the block number of the recorded watermark ID hash or the exact owner's watermark ID hash that has been extracted and hashed from the received image. We use one of these two pieces of information to fetch the saved watermark from the blockchain. The final step is to compare the watermark ID hash that is extracted from the image and the watermark ID hash that is recorded into the blockchain; if they match, then the image is authentic.

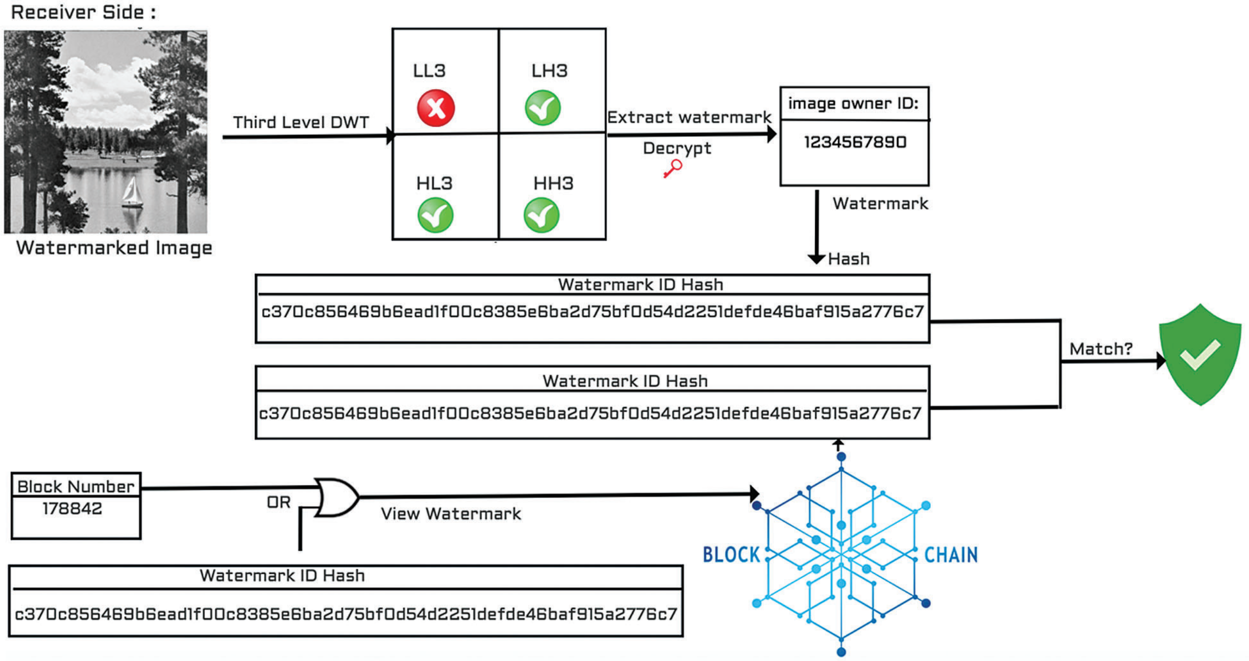

Figure 2: Secure watermark extraction

Blockchain is used to validate the authenticity of the watermark such that no third party is involved in the authentication process. In the proposed approach, AES-128 encryption is used to encrypt the watermark before embedding the watermark into the input image, as shown in Fig. 1.

3.1 Watermark Embedding Process

The watermark embedding consists of applying third-level DWT on the original image I_i. I_i is divided into 4 × 4 non-overlapping blocks. Then the watermark is encrypted using AES encryption with a secret key. The embedding strength E is initialized to 5. The difference D is calculated using the following equation:

$$D = | \ B_i(i,j) - B_{i+1}(k,l) \ | \tag{1}$$

The difference D is calculated for all the watermark W_b and the watermark is embedded into I_i. The embedding algorithm is specified in Alg. 1, where B_i is ith block of wavelet coefficients and Bin_i is i^{th} embedding bit.

SHA-256 is applied to the watermark before saving it into the blockchain in the embedding phase as shown in Fig. 1, and in the extraction phase as shown in Fig. 2. After extracting the encrypted watermark from the input image and decrypting the watermark, we apply SHA-256 to the watermark. SHA-256 hashing is one of the most secure ways to secure digital information. It is a mathematical process that generates 256-bit random letters and numbers from any input.

Algorithm 1: Embedding

```
for $i$ =1 to i = no. of embedding bits do
        $M_1 = [B_i]$
        $M_2 = [B_{i+1}]$
    $P_1, P_2 = 0$
    if $Bin_i$ =0 then
        if $(M_1 - M_2) > E$ then
            $B_i = M_1, B_{i+1} = M_2$
        else
            while $(M_1 - M_2) < E$ do
                    $M_1 = [B_i] + P_1$
                    $M_2 = [B_{i+1}] - P_2$
                increment $P_1, P_2$
            endwhile
        endif
    else
endfor
$Bini_i$ =1
if $(M_1 - M_2) < E$ then
    $B_i = M_1, B_{i+1} = M_2$
else
    while $(M_1 - M_2) > E$ do
            $M_1 = [B_i] - P_1$
            $M_2 = [B_{i+1}] + P_2$
        increment $P_1, P_2$
    endwhile
    $B_i = M_1, B_{i+1} = M_2$
endif
```

3.2 Watermark Extraction Process

The watermarked image is decomposed into 4 × 4 blocks. The difference between the pixels B_i and B_{i+1} of the neighboring blocks is calculated using Eq. 1. The extraction algorithm is specified in Alg. 2, where B_i is i^{th} block of wavelet and BP_i is i^{th} extracted bit.

Algorithm 2: Watermark extraction

```
for $i$ =1 to $i$ = no. of extraction bits do
        $M_1$= [ $B_i$ ]
        $M_2$ = [ $B_{i+1}$]
    if $(M_1 - M_2) < E$ then
        $BP_i$ =0
    else
        $BP_i$ =0
    endif
endfor
```

4 Experimental Results

The experiments were conducted using gray-scale images of size 512 × 512 pixels and 256 × 256 pixels from USC SIPI image database [20]. In the experiments, 242 images are used. The watermark is a 10-digit ID number that is repeated thrice in the image. The reason for repeating the watermark is to increase the security and robustness of the watermark. PSNR, NCC, SSIM, and BER are used to evaluate the watermarking approach.

Peak Signal-to-Noise Ratio (PSNR) is given by Eq. 2.

$$PSNR = 10\ log \frac{\max(I_i(i,j), I_\omega(i,j))}{\sum_{i=1}^{M}\sum_{j=1}^{N} I_i(i,j) \times\ I_\omega(i,j)} \tag{2}$$

where I_i is the original image and I_ω is the watermarked image.

Normalized correlation coefficient (NCC) is given by Eq. 3.

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W_i - \overline{W_j}\right)\left(W_\omega - \overline{W_\omega}\right)}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W_i - \overline{W_i}\right)^2\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W_\omega -\ \overline{W_\omega}\right)\right.}} \tag{3}$$

M is the number of rows of the image, N is the number of columns, W is the original watermark, W_ω extracted watermark, $\overline{W_i}$ = mean (W_i), and $\overline{W_\omega}$ = mean (W_ω).

The Structural Similarity Matrix is given by Eq. 4.

$$SSIM(M,N) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu^2{}_X + \mu^2{}_Y + C_1)(\sigma^2{}_X\ + \sigma^2{}_Y\ + C_2)} \tag{4}$$

where μ_x is the average of I_i, μ_y is the average of I_ω, σ_x^2 is the variance of I_i, σ_y^2 is the variance of I_ω, and σ_{xy} the covariance of I_i and I_ω. C1 = (k1L)2 and C2 = (k2L)2 two variables used to stabilize the division with the weak denominator. L is the dynamic range of the pixel values and k1 = 0.01 and k2 = 0.03 by default.

Bit Error Rate (BER) is given in Eq. 5.

$$BER = \frac{\text{Number of errors}}{\text{Number of bits in watermark}} \tag{5}$$

4.1 Perceptual Quality Analysis—USC SIPI Database

Tab. 1 shows the comparison between results when embedding into different wavelet sub-bands. The comparison is carried out to determine the effect of embedding the watermark into each region on the perceptibility metrics. Embedding into all the three third-level high frequency regions has comparable results to embedding in other sub-bands with the embedding strength 1. The results of embedding into all the three third-level high frequency sub-bands give PSNR 48.147, SSIM 0.997, NCC 0.999, and BER 0.073.

Table 1: PSNR, SSIM, NCC, BER of the USC SIPI images database using the secure method on third-level sub-bands

Region	PSNR dB	SSIM	NCC	BER
LH3	47.539	0.997	0.999	0.083
HL3	45.114	0.995	0.999	0.087
HH3	47.024	0.997	0.999	0.084
LH3, HL3	42.946	0.992	0.998	0.132
LH3, HH3	44.432	0.994	0.998	0.124
HL3, HH3	47.389	0.997	0.999	0.078
LH3, HL3, HH3	48.147	0.997	0.999	0.073

Tab. 2 shows a comparison between the results of different sample images from USC SIPI image database using the proposed method. We see that the PSNR values range from 42.347 dB to 54.899 dB. The SSIM value is between 0.989 and 0.998. NCC value is between 0.998 and 0.999. BER has values from 0.020 to 0.117.

Table 2: PSNR, SSIM, NCC, BER of sample images from USC SIPI database using the proposed method

Test Image	PSNR dB	SSIM	NCC	BER
Baboon	42.347	0.996	0.998	0.11
Girl	43.083	0.989	0.999	0.117
Pepper	50.915	0.998	0.999	0.047
House	42.877	0.992	0.999	0.1
Airplane	47.938	0.997	0.999	0.051
Splash	54.899	0.998	0.999	0.031
Lake	47.083	0.997	0.999	0.075
Blocks	54.477	0.997	0.999	0.101
Man	44.354	0.993	0.999	0.09
Waves	50.759	0.997	0.999	0.02
Bricks	45.958	0.996	0.999	0.102
Average	47.699	0.995	0.999	0.077

E factor is the strength of watermark embedding. Tab. 3, shows the results when applying different strength values. It also shows that whenever the value gets higher, the performance metrics get lower. The best performance metrics in terms of invisibility are achieved for E value of 1. The PSNR value, in this case, is 48.147 dB, SSIM is 0.997, NCC is 0.999, and BER is 0.073.

Table 3: PSNR, SSIM, NCC, and BER of the USC SIPI images database using different values of E

Strength Value E	PSNR dB	SSIM	NCC	BER
1	48.147	0.997	0.999	0.073
5	47.149	0.996	0.999	0.085
10	46.800	0.996	0.999	0.090
15	46.215	0.996	0.999	0.093
20	45.593	0.995	0.999	0.095
25	45.017	0.993	0.999	0.100
30	44.365	0.991	0.998	0.099
Average	46.183	0.994	0.998	0.090

The test and analysis of the proposed watermarking approach show acceptable results on the performance metrics related to imperceptibility. The testing of the proposed watermarking method is also examined using changes and attacks such as addition of noise, compression, and filtering on the watermarked images. Tab. 4 shows the tests and results of the proposed watermarking method using different attacks such as additive white Gaussian, salt and pepper, speckle, and Poisson noise. JPEG compression, median filtering, mean filtering, and Gaussian filtering attacks were also applied to the watermarked images. From the results we get from applying these different attacks, we can see that JPEG compression with 90% has PSNR 38.469, SSIM 0.968, NCC 0.994, and BER 0.245. The calculated metrics drop as more compression is applied to the watermarked images. On the other hand, when Gaussian noise is added to the image, the lowest results of PSNR 13.144, SSIM 0.176, NCC 0.541, and BER 0.464 are obtained. This signifies the sensitivity of the watermarking algorithm to Gaussian noise.

From Tabs. 1–4, we can conclude that the watermarking algorithm is not very robust against attacks. However, it has better performance in terms of imperceptibility which is a desired trait of image authentication approaches.

4.2 Perceptual Quality Analysis—MedPix Database

To demonstrate the effectiveness of the proposed watermarking approach on medical images, we used the MedPix database [21]. It is a freely available online database of medical images. Gray-scale chest X-ray images of size 256 × 256 are considered as the host images. In the experiments, we used 200 medical images. The watermark is a 10-digit ID number that is repeated three times in the image. A sample image from the database after watermarking is shown in Fig. 3b. The original image is shown in Fig. 3a.

Test results of sample test images that are used for the experiments are given in Tab. 5. The highest PSNR and SSIM values for the images are 60.339 and 0.999, respectively. The NCC value is the same for all images, 0.999 and BER has the lowest value, 0.008. The lowest PSNR value is 54.920 and the lowest SSIM value is 0.997.

PSNR and SSIM values decrease when using high embedding strength, as shown in Tab. 6. On the other hand, the NCC value remains the same. The BER has the highest value when E is 1.

Table 4: PSNR, SSIM, NCC, BER of the USC SIPI images database under different attacks

Attacks	Value	PSNR dB	SSIM	NCC	BER
JPEG	**10%**	27.741	0.763	0.942	0.346
	50%	32.678	0.902	0.979	0.299
	80%	35.623	0.943	0.989	0.272
	90%	38.469	0.968	0.994	0.245
Median filter	**3 × 3**	30.978	0.859	0.966	0.257
	7 × 7	25.455	0.618	0.89	0.33
	9 × 9	24.145	0.55	0.855	0.343
Mean filter	**3 × 3**	28.83	0.828	0.953	0.308
	7 × 7	23.88	0.566	0.857	0.357
	9 × 9	22.778	0.498	0.816	0.368
Salt and pepper	**0.01**	25.246	0.817	0.918	0.085
	0.03	20.509	0.583	0.81	0.094
	0.05	18.285	0.443	0.732	0.102
Speckle noise	**0.01**	25.901	0.674	0.915	0.377
	0.05	19.128	0.406	0.758	0.433
Poisson noise	**–**	27.256	0.711	0.938	0.359
Gaussian noise	$\mu = 0$ $\sigma^2 = 0.01$	17.264	0.395	0.801	0.447
	$\mu = 0$ $\sigma^2 = 0.05$	13.144	0.176	0.541	0.464
Gaussian filter	**3 × 3**	38.098	0.976	0.994	0.227
	9 × 9	38.073	0.976	0.994	0.228
Average		26.074	0.667	0.876	0.300

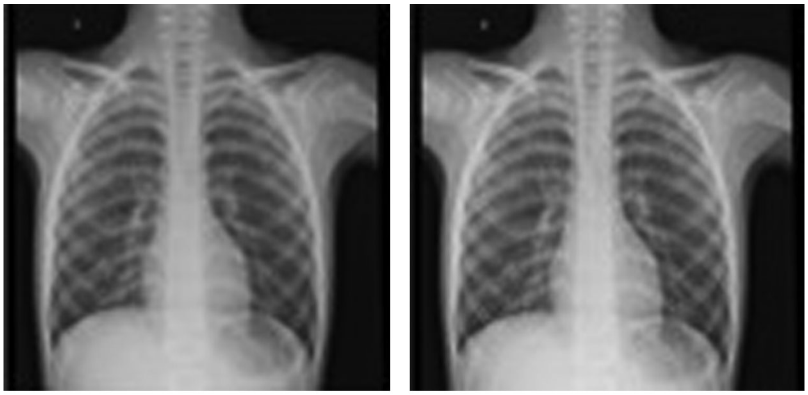
(a) (b)

Figure 3: Medical image—chest X-Ray a. Original chest X-ray image b. Watermarked chest X-ray image

Table 5: PSNR, SSIM, NCC, and BER of the sample images from the MedPix database

Test Image	PSNR dB	SSIM	NCC	BER
Chest X-ray 1	55.319	0.998	0.999	0.039
Chest X-ray 2	55.517	0.998	0.999	0.036
Chest X-ray 3	55.868	0.998	0.999	0.038
Chest X-ray 4	54.987	0.997	0.999	0.047
Chest X-ray 5	54.920	0.998	0.999	0.041
Chest X-ray 6	55.929	0.998	0.999	0.037
Chest X-ray 7	55.319	0.998	0.999	0.039
Chest X-ray 8	58.365	0.999	0.999	0.020
Chest X-ray 9	58.273	0.999	0.999	0.010
Chest X-ray 10	56.455	0.998	0.999	0.024
Chest X-ray 11	60.339	0.999	0.999	0.008
Chest X-ray 12	58.365	0.999	0.999	0.015
Average	56.643	0.998	0.999	0.030

Table 6: PSNR, SSIM, NCC, and BER of the MedPix database for different values of E

E strength value	PSNR dB	SSIM	NCC	BER
1	55.981	0.998	0.999	0.045
5	55.798	0.998	0.999	0.035
10	55.431	0.998	0.999	0.036
15	54.809	0.997	0.999	0.037
20	54.137	0.997	0.999	0.038
25	53.519	0.996	0.999	0.038
30	52.715	0.996	0.999	0.038
Average	54.627	0.997	0.999	0.038

Tab. 7 shows the PSNR, SSIM, NCC, and BER values for images from the MedPix database under different attacks. JPEG compression, median filter, mean filter, salt and pepper noise, speckle noise, additive white Gaussian noise, and Gaussian filter attacks are applied to the watermarked images. The medical images were impacted the most by Gaussian noise and least by Gaussian filter attack.

4.3 Blockchain Experimental Results

To measure the performance of the blockchain, we use the CPU time for every node. We use Grafana to measure CPU time. After successfully recording the watermark into the blockchain, we used the Ethereum lite explorer and Grafana for analyzing the data recorded in the blockchain.

Table 7: PSNR, SSIM, NCC, and BER of the MedPix database under different attacks

Attacks	Value	PSNR dB	SSIM	NCC	BER
JPEG	10%	33.694	0.828	0.995	0.293
	50%	39.463	0.928	0.998	0.235
	80%	42.069	0.957	0.999	0.208
	90%	44.008	0.972	0.999	0.186
Median Filter	3×3	41.692	0.952	0.999	0.172
	7×7	36.593	0.894	0.997	0.234
	9×9	35.132	0.879	0.996	0.245
Mean Filter	3×3	37.297	0.942	0.997	0.209
	7×7	32.581	0.868	0.993	0.257
	9×9	31.335	0.847	0.991	0.268
Salt and Pepper	0.01	25.163	0.723	0.969	0.038
	0.03	20.401	0.405	0.913	0.047
	0.05	18.168	0.246	0.862	0.057
Speckle Noise	0.01	25.173	0.446	0.969	0.367
	0.05	18.45	0.214	0.874	0.421
Poisson Noise		27.055	0.493	0.979	0.35
Gaussian Noise	$\mu = 0$ $\sigma^2 = 0.01$	13.837	0.043	0.702	0.453
	$\mu = 0$ $\sigma^2 = 0.05$	13.213	0.044	0.708	0.458
Gaussian Filter	3×3	47.92	0.991	0.999	0.122
	9×9	47.876	0.991	0.999	0.123
Average		31.556	0.683	0.946	0.237

4.3.1 Ethereum lite explorer

Ethereum lite explorer is an application used to connect to Ethereum javascript object notation remote procedure call compatible node which is a private Ethereum explorer that does not need any servers or any third party to show blockchain data. To display blockchain data, we could search the Ethereum lite explorer by entering the block number, transaction hash, and address. Ethereum lite explorer shows detailed information related to the block. A list of information as shown for a certain block is given in Tab. 8.

4.3.2 Grafana

Grafana [22] is used to visualize and analyze data. It allows to query, visualize, alert on, and explore metrics. It is used as a tool to chart Time-Series DataBase (TSDB) data into clear graphs. It represents the block time graph that shows the date of the time in seconds when the block has been registered, the maximum and minimum time taken by the node to carry out a job, the average time calculated, and the current time. Tab. 9, represents values of the block time used for certain nodes. This table only shows the details of bootnode, Rpcnode, and validators nodes indicating acceptable time taken to perform tasks related to the proposed watermarking approach.

Table 8: Information shown in Ethereum lite explorer

Block information	Value
Block Number	#452332
Time	7 hours ago
Hash	0xfb5…
Parent	0xf4d…
Nonce	0x000000000
Size	1,052 bytes
From	0xcf4……
To	0x0fa……
Value (ETH)	0.000

Table 9: Block time

Node	Block Time (seconds)			
	Min	Max	Avg	Current
Bootnode	1.9	2.0	2.0	2.0
Rpcnode	1.9	2.0	1.9	1.9
Validator2	1.9	2.0	2.0	2.0
Validator3	1.9	2.0	2.0	1.9
Validator4	1.9	2.0	2.9	2.0

5 Comparisons With State-of-the-art Methods

Tab. 10 shows a comparison between the most relevant papers representing image authentication using watermarking or blockchain. As we can see from Tab. 10, the proposed method introduced a new method that combines watermarking and blockchain to serve the main purpose of image authentication, security, and imperceptibility all together while presenting a reasonable high PSNR. The results shown in Tab. 10 are carried out on the USC SIPI database. Tab. 11 shows a comparison between the most relevant papers representing image authentication using watermarking or blockchain for medical images using the MedPix image database.

This comparison is based on six categories: the database that has been used during the testing, the methodology, PSNR, blind, which refers to the watermarking mechanism if it requires the original image during the extraction phase, authentication method, security method, and limitation of the work. We compared the proposed method with other methods in terms of watermarking methods and their security.

The proposed work is compared with Bhowmik and Feng [23], Meng [24], and with other methods presented in [17–19] that have been tested using the same database. The average values of PSNR indicate the efficiency of the proposed approach to preserve the invisibility between the original and watermarked images. The proposed approach demonstrates better performance than state-of-the-art in several categories. The use of the blockchain to accomplish authentication without the involvement of a trusted third party with acceptable levels of PSNR is a special advantage of the proposed approach.

Table 10: Comparisons of the proposed approach using the USC SIPI database with state-of-the-art methods

Paper	Block size	Dataset	Methodology	PSNR dB	Blind	Authentication mechanism	Security mechanism	Limitation
[17]	4 × 4	USC SIPI and CVG-UGR database	Schur decomposition spatial domain watermarking	40.000	√	–	–	Low results Security and authentication mechanism limitation
[18]	4 × 4 and 8 × 8	USC SIPI and ILSVRC2016 database	Rotating vector semi-fragile watermarking	41.070	√	Rotating vector watermarking	–	Low results
[19]	–	USC SIPI, CVG-UGR image database	(LWT),(SVM) watermarking	43.880	√	–	–	Lower PSNR results
[23]	–	Standard dataset provided by Christlen et al.	Blockchain and self embedding watermarking	–	√	Blockchain	–	No performance watermarking results
[24]	–	–	Watermarking, blockchain, perceptual hash function, QR code, and IPFS	–	–	Blockchain	Perceptual hash function cryptographic hash function.	No performance evaluation values
Proposed algorithm	4 × 4	USC SIPI image database	DWT watermarking and blockchain	48.147	√	Blockchain	AES watermark encryption + watermark hash	–

Table 11: Comparison of the MedPix medical image database with state-of-the-art methods

Paper	Dataset	Methodology	PSNR dB	Blind	Authentication mechanism	Security mechanism	Limitation
[25]	MRI images	Spatial domain watermarking	41.730	X	–	Watermarking	Non blind
[26]	CT Scan images	DCT watermarking	41.152	√	–	Watermarking	Low performance
[27]	MRI, CT Scan and Ultrasound images	DWT and DCT watermarking	37.042	X	–	Hamming error, correction code and encryption	Low performance
[28]	MRI images	DWT, DCT and SVD watermarking	35.840	X	–	Encryption	Low performance
[29]	CT, MRI and ultrasound images	Region of Non-Interest (RONI)	38.010	X	–	–	Non blind Low performance
Proposed algorithm	MedPix image database	DWT watermarking and blockchain	55.981	√	Blockchain	AES watermark encryption + watermark hash	–

Tab. 11 shows the comparison with other medical image databases using the previously mentioned categories. The proposed method has reached an average PSNR of 55.981, which is the highest value compared with other methods. All the compared works have one or more limitations: lower PSNR value compared to the proposed method, absence of authentication mechanism, and absence of security mechanism. According to our review of the state-of-the-art, the proposed medical image watermarking approach is the first method that demonstrates an effective solution to the medical image authentication problem using the blockchain, thus removing the need for trusted third parties.

6 Conclusion

Image authentication is an important field that is carried out using different techniques. In this paper, we used watermarking and blockchain combined together to achieve image authentication. Image authentication scheme has been introduced using the technologies of watermarking in the third-level DWT, AES encryption, SHA-256 hashing, and blockchain. Our consideration is to authenticate and secure the digital images from manipulation. Our approach has five different steps to follow. Encrypting the watermark using AES encryption with a secret key. Embedding the encrypted watermark into the three middle frequency regions of the third-level DWT. Taking the same watermark and hashing to save into the blockchain. At the extraction stage, the watermark is extracted from the host image, the encrypted watermark is decrypted using the same secret key. The decrypted watermark is hashed using SHA-256 for comparing it with the hashed watermark that is saved in the blockchain. From the blockchain, we acquire the hash of the watermark or the block number of the transaction that contains the saved watermark. After getting the hash of the watermark we compare it with the watermark that is extracted from the image. If the comparison matches then it is an authentic image, if it does not match then the image has potentially been attacked and is not authentic. For the experimental tests, we used USC SIPI database and MedPix medical database with different image sizes. Our results have shown that the proposed watermarking approach gives the best performance compared to the state-of-the-art works. In the future, the proposed technique could be tested with other images such as MRI, CT, ultrasound, and other kinds of medical images. Also, the proposed algorithm can be applied on color images as future work.

Acknowledgement: This Project was funded by the National Plan for Science, Technology and Innovation (MAARIFAH), King Abdulaziz City for Science and Technology, Kingdom of Saudi Arabia, Award Number (13-INF2114-02).

Funding Statement: This Project was funded by the National Plan for Science, Technology and Innovation (MAARIFAH), King Abdulaziz City for Science and Technology, Kingdom of Saudi Arabia, Award Number (13-INF2114-02).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] O. Nafea, S. Ghouzali, W. Abdul and E. Qazi, "Hybrid multi-biometric template protection using watermarking," *Computer Journal*, vol. 59, no. 9, pp. 1392–1407, 2016.

[2] S. Ghouzali and W. Abdul, "Private chaotic biometric template protection algorithm," in *IEEE Second Int. Conf. on Image Information Processing (ICIIP-2013)*. Shimla, India, 655–659, 2013.

[3] W. Abdul, O. Nafea and S. Ghouzali, "Combining watermarking and hyper-chaotic map to enhance the security of stored biometric templates," *Computer Journal*, vol. 63, no. 3, pp. 479–493, 2020.

[4] A. Haouzia and R. Noumeir, "Methods for image authentication: A survey," *Multimedia Tools and Applications*, vol. 39, no. 1, pp. 1–46, 2008.

[5] S. Bennett, *Blockchain: A guide to Understanding Blockchain*. Newyork, USA: The Cryptomasher Series, 2017.

[6] M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, pp. 6–9, 2016.

[7] H. Hou, “The application of blockchain technology in E-government in China,” in *IEEE, 26th Int. Conf. on Computer Communication and Networks*. Vancouver, BC, Canada, 1–4, 2017.

[8] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah *et al.,* “Blockchain technology the identity management and authentication service disruptor: a survey,” *Int. Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 4–2, pp. 1735–1745, 2018.

[9] W. Wang, N. Hu and X. Liu, “BlockCAM: A blockchain-based cross-domain authentication model,” in *IEEE Third Int. Conf. on Data Science in Cyberspace (DSC)*. Guangzhou, China, 896–901, 2018.

[10] B. Liu, Z. Chen, Y. Zhang, L. Xiong, X. Yang *et al.,* “A new group-to-group authentication scheme based on PUGs and blockchain,” in *IEEE 4th Int. Conf. on Signal and Image Processing*. Wuxi, China, 279–283, 2019.

[11] M. Thakur, “Authentication, authorization and accounting with Ethereum blockchain,” 61, University of Helsinki, Finland, 2017.

[12] L. Xiong, F. Li S. Zeng, T. Peng and Z. Liu, “A blockchain-based privacy-awareness authentication scheme with efficient revocation for multi-server architectures,” *IEEE Access*, vol. 7, pp. 125840–125853, 2019.

[13] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos and G. Das, “Proof-of-authentication for scalable blockchain in resource-constrained distributed systems,” in *IEEE Int. Conf. on Consumer Electronics (ICCE)*. Las Vegas, NV, USA, 1–5, 2019.

[14] G. Zyskind and O. Nathan, “Decentralizing privacy: Using blockchain to protect personal data,” in *IEEE Security and Privacy Workshops*, pp. 180–184, 2015.

[15] D. Drescher, “using the blockchain, Blockchain basics: A non-technical introduction in 25 steps, Frankfurt am main, Germany, 2017, [online]. Available: http://www.softouch.on.ca/kb/data/Blockchain%20Basics.pdf

[16] F. Chen, H. He and Y. Huo, “Self-embedding watermarking scheme against JPEG compression with superior imperceptibility,” *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 9681–9712, 2017.

[17] Q. Su, Z. Yuan and D. Liu, “An approximate schur decomposition-based spatial domain color image watermarking method,” *IEEE Access*, vol. 7, pp. 4358–4370, 2019.

[18] J. Fu, J. Mao, D. Xue and D. Chen, “A watermarking scheme based on rotating vector for image content authentication,” *Soft Computing*, vol. 24, no. 8, pp. 5755–5772, 2020.

[19] M. Islam, A. Roy and R. H. Laskar, “SVM-based robust image watermarking technique in LWT domain using different sub-bands,” *Neural Computing and Applications*, vol. 32, no. 5, pp. 1379–1403, 2020.

[20] USC university of Southern California, “The USC-SIPI Image Database,” 2019. [Online]. Available at: http://sipi.usc.edu/database.

[21] National library of medicine, “MedPix image database,” 2020. [Online]. Available at: https://medpix.nlm.nih.gov/.

[22] Grafana Labs, “Grafana,” (2020). [online]. Available at: https://grafana.com/.

[23] D. Bhowmik and T. Feng, “The multimedia blockchain: a distributed and tamper-proof media transaction framework,” in *IEEE 22nd Int. Conf. on Digital Signal Processing*. London, UK, 1–5, 2017.

[24] Z. Meng, T. Morizumi, S. Milyata and H. Kinoshita, “Design scheme of copyright management system based on digital watermarking and blockchain,” in *IEEE 42nd Int. Conf. on Computer Software and Applications*. Tokyo, Japan, 359–364, 2018.

[25] S. M. Mousavi, A. Naghsh, A. A. Manaf and S. A. R. Abu-Bakar, “A robust medical image watermarking against salt and pepper noise for brain MRI images,” *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 10313–10342, 2017.

[26] S. A. Parah, J. A. Sheikh, F. Ahad, N. A. Loan and G. M. Bhat, “Information hiding in medical images: A robust medical image watermarking system for E-healthcare,” *Multimedia Tools and Applications*, vol. 76, no. 8, pp. 10599–10633, 2017.

[27] A. Sharma, A. K. Singh and S. P. Ghrera, “Robust and secure multiple watermarking for medical images,” *Wireless Personal Communications*, vol. 92, no. 4, pp. 1611–1624, 2017.

[28] A. Anand and A. K. Singh, “An improved DWT-SVD domain watermarking for medical information security,” *Computer Communications*, vol. 152, no. 3, pp. 72–80, 2020.

[29] N. E. H. Goléa and K. E. Melkemi, “ROI-based fragile watermarking for medical image tamper detection,” *Int. Journal of High-Performance Computing and Networking*, vol. 13, no. 2, pp. 199–210, 2019.