This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3028612, IEEE Transactions on Industrial Informatics

DWFCAT: Dual Watermarking Framework for Industrial Image Authentication and Tamper Localization

***Abstract*—**Image data received through various sensors is of significant importance in Industry 4.0. Unfortunately, this data is highly vulnerable to various malicious attacks during its transit to the destination. Though the use of Pervasive Computing (PEC) with the Internet of Things (IoT) has solved various issues like latency, proximity, and real-time processing, but the security and authentication of data between nodes is still a significant concern in PEC based Industrial IoT (IIoT) scenarios. In this paper, we present "DWFCAT", a dual watermarking framework for content authentication, and tamper localization for industrial images. Robust and fragile watermarks along with overhead bits related to the cover image for tamper localization are embedded in different planes of the cover image. We have used a Discrete Cosine Transform (DCT) coefficients and exploited their energy compaction property for robust watermark embedding. We make use of a 4-point neighborhood to predict the value of a predefined pixel and use it for embedding the fragile watermark bits in the spatial domain. Chaotic and Deoxyribonucleic Acid **(**DNA**)** encryption is used to encrypt the robust watermark before embedding to enhance its security. The results indicate that DWFCAT can withstand a range of hybrid signal processing and geometric attacks such as Gaussian noise, salt, and pepper, JPEG compression, rotation, low pass filtering, resizing, cropping, sharpening, and histogram equalization. Experimental results prove that the DWFCAT is highly efficient compared to various state-of-the-art approaches for authentication and tamper localization of industrial images.

***Index Terms*—**Pervasive Edge Computing, IIoT, Authentication, Tamper localization, Watermarking.

I. Introduction

THE development of 5G networks is envisioned to meet the extreme capacity and performance demands. Emerging technologies such as Network Functions Virtualization (NFV), Software-Defined Networking (SDN), Pervasive Edge Computing (PEC), Internet of Things (IoT), and 5G platforms are supposed to be the main pillars of Industry 4.0. PEC is a concept wherein services related to cloud and resources are bought nearer to the user, to meet the requirements of location awareness, low latency, and mobility support [1, 2]. PEC envisions integrating computing, storage, and networking resources with the base station. Unfortunately, from a security point of view, PEC is troublesome in the distributed environment, given the fact that the data handling capacity of various devices is not as secure as a centralized system [3, 4]. This necessitates the development of new security solutions to cater to the needs of security and privacy protection in an Industry [5, 6, 7].

More recently, a considerable booming of visual sensors has been seen in IoT systems due to their ability to provide rich and versatile information [8, 9]. To securely exchange data in these environments with high network insecurity, approaches such as encryption, steganography, digital watermarking, and digital signatures are used [10, 11, 12]. Digital watermarking has been found to be as a better choice to address the issues like security, authentication tamper detection and localization of tampered data. Besides watermarking technology could enable proper identification of the node transmitting data in a PEC and IoT driven distributed environment [13]. Most of the reported work on watermarked technology using industrial imagery is based on grayscale images. However, the present-day practical scenarios like Visual-IoT (VIoT) and Smart cities that include the deployment of camera sensors generally provide color information that needs to be secured [14, 15]. The real-world color images are mostly represented by RGB color space because it is a natural space consisting of correlated red, green, and blue channels [16]. The other key color model YCbCr breaks an image into the luminance component (Y), and two chrominance components, i.e., Cb and Cr based on visual information.

Robustness to cyber-attacks, authentication of data and, computational efficiency are important requirements for secure data exchange in an Industrial-IoT (IIoT) system. A comprehensive literature survey reveals that for data authentication, fragile watermarking schemes are predominantly used [17] but they are not capable of tamper localization. Some other schemes such as [18] can locate tampered areas but have low imperceptibility. Besides, most of the fragile watermarking schemes are non-blind and need an original watermark for accomplishing the purpose of authentication. To achieve high robustness many state-of-art schemes like [21, 22, 23, 27, 28] make use of dual transforms like DCT-DWT for embedding the information but are computationally complex due to the use of dual transformation, thus can't be used in real-time IIoT applications. Also, the mentioned schemes [21, 22, 23, 27, 28] have not been analyzed for simultaneous attacks, a very important requirement in the IIoT setup.

In this work, we present DFWCAT utilizing a single transform (DCT) and an innovative embedding strategy, as such resulting in a highly robust, yet computationally efficient system; a better choice for real-time implementation required in IIoT. Embedding in transformation coefficients, leaving the DC coefficient of each block and utilizing the block coefficient correlation mechanism, provides better imperceptivity and higher robustness to singular and simultaneous attacks. To ensure content authentication while maintaining imperceptibly, we have employed a modified prediction error expansion method to embed fragile watermark bits in the spatial domain. The fragile watermark is capable of localizing the tampered region in addition to authenticate the received content. Besides, DWFCAT uses YCbCr color space instead of RGB color space because it offers high robustness and the extraction is better after Gaussian noise and JPEG compression attacks. The security of the embedded watermarks has been taken care of utilizing Chaotic and DNA encryption.

To summarize the DWFCAT presents a secure framework for authentication, tamper localization, and copyright

protection of industrial images. Robust watermark is embedded in the Y channel and fragile watermark in the Cb channel along with additional overhead bits for tamper localization. The major contributions of this work are multi-fold and are presented as:

- DWFACT takes into consideration the characteristics of the Human Visual System (HVS) for embedding the watermark information in a cover media. We have developed an innovative embedding procedure by exploiting the energy compaction property of DCT to retain the image quality and achieve high robustness despite hybrid attacks in an IIoT environment.
- Fragile watermarks are embedded by exploiting a high correlation between adjacent pixels to ensure data authentication and tamper localization.
- To ensure the security of embedded watermarks, DWFCAT doubly encrypts both robust and fragile watermarks using Chaotic and DNA encryption.
- DWFCAT is designed as a blind technique, i.e., neither cover image nor original watermark is needed for the extraction of the embedded information.

The remaining portion of the paper has been arranged as follows. Prior associated work has been discussed briefly in Section II. Watermark preparation has been discussed in Section III. The proposed DWFCAT framework has been discussed in detail in Section IV. Section V presents the experimental results. The analysis of results has been presented in section VI. The paper has been concluded in section VII.

II. Related Work

The enormous data production and exchange have put forward many limitations on centralized cloud computing systems in an Industrial IoT setup. In this scenario, PEC is promised to be an answer to these limitations. Although PEC successfully counters most of the limitations of centralized cloud computing systems, data security, and privacy issues have evolved to be a major challenge in this distributed environment [19]. Nonstop research in areas associated with providing security and privacy protection is being undertaken by researchers all over the world. Among different means of providing security to Industrial data, digital watermarking has been established to be adequately useful. We can classify watermarking techniques based on the desired robustness of the embedded watermark into “fragile watermarking” [17, 18] and “robust watermarking” [20, 21]. The two domains which can be used for embedding watermark bits are spatial and transform domains. Less complexity and high embedding capacity are the two main advantages associated with spatial domain schemes while transform-domain schemes are characterized by high robustness. It has been found that the transform domain is apt for embedding a robust watermark and the spatial domain is apt for embedding a fragile watermark. Fragile watermarking finds application in content authentication of cover media. Since fragile watermark should be sensitive to even minute changes in cover media it is usually embedded in a spatial domain. In Chang et.al [17] a novel fragile watermarking framework has been put forward wherein the images were secluded and the scheme proposed was able to identify any alteration to an image; using a combination of hamming code and a two-pass logistic map. In Zang and Wang [18] a scheme has been proposed wherein they are capable of getting back the original image from the one being tampered. They have used a reversible technique for embedding watermark extracted from the original image into the cover image. Deep learning (DL) based authentication framework has been presented in [20]. The authors have discussed Artificial Intelligence (AI) and Machine Learning (ML) based approaches for authentication. Issues about real-time implementation in AI and ML have been highlighted and a new AI framework based on ML and DL has been presented.

In the area of robust watermarking, it is still a challenge to get high robustness and high imperceptibility simultaneously. As a result, there is always a tradeoff between the above-mentioned properties. Abraham et al. [16] have proposed a novel robust watermarking framework based on the spatial domain. In this paper, a robust watermark has been embedded in the spatial domain rather than in the transform domain. The watermark information is embedded by spreading it gradually over some region of pixels. Although the scheme offers high imperceptibility and good robustness, there is no provision for the security of the watermark. The majority of the current robust watermarking schemes use hybrid transform domain techniques to increase the robustness of the watermarking schemes. In Feng et al. [21] a blind robust watermarking scheme has been proposed which is a blend of DWT and DCT. Watermark is first scrambled using Arnold transform and then embedded in spread spectrum pattern with the help of pseudo-random series. The mid-frequency DCT coefficients of LL sub-band obtained after using DWT have been used for embedding. However, the use of dual transformations results in high computational cost.

Different watermarks are being embedded into the same cover image for accomplishing several goals simultaneously. These techniques may incorporate a blend of two or more watermarks depending on the application for which a concerned technique is designed. In Kang et al. [22] a blind composite watermarking framework using DWT and Discrete Fourier Transform (DFT) has been proposed. Investigational works in this field suggest that their scheme is robust to the common signal processing attacks but poor to geometric attacks. Also, the use of dual transform makes the scheme computationally more complex rendering it unsuitable for real-time applications. Lin et al. [23] have proposed a dual watermarking framework focusing on copyright protection only. The scheme embeds a visible watermark in the spatial domain and an invisible watermark in the frequency domain by using the just notable distortion technique. Shi et. al. [24] have proposed a semi-fragile dual watermarking scheme using region adaption. The embedding capacity is increased and blind extraction is made possible in the scheme by use of a status code technology. In Roy et al. [25] multiple watermarking schemes have been presented which make use of DCT and

reiteration code. The strength of the scheme is established after making the watermarked image pass through geometric attacks, enhancement technique attacks, and JPEG compression attacks. Lusson et. al. [26] proposed a dual robust watermarking scheme wherein one watermark has been embedded into the RGB and other in YCbCr color space to increase the robustness of watermarks embedded. The scheme, however, requires the original watermark for extracting the watermark bits. The dual watermarking schemes [23-26] focus on copyright protection only. No attention has been given to image authentication and security of watermarks embedded. Su et al. [27] proposed a dual watermarking scheme based on Singular Value Decomposition (SVD). The scheme exploits the correlation between different elements of orthogonal matrix U via SVD for embedding the watermarks. However, the scheme offers weak imperceptivity. Lui et.al [28] make use of DWT for embedding a robust watermark in YCbCr color space and modified version of Least Significant Bit (LSB) substitution for embedding a fragile watermark in RGB color space. The scheme shows good robustness but there is no provision for securing the robust watermark.

The various dual watermarking schemes discussed above do not address the issues of authentication, copyright protection, tamper detection, and localization simultaneously. Also, the prime issue is that these techniques have been tested only for a singular attack, no testing has been done for real-time scenarios where multiple attacks may occur at the same time. In this paper, we have come up with a dual watermarking scheme that addresses all the said issues simultaneously and is as such suitable for real-time applications and could also prove advantageous in a PEC and 5G based IoT scenario.

III. Watermark Preparation

The security of the data can get compromised if an unauthorized user cracks the algorithm used for embedding the watermark information [8]. To make the proposed technique more secure, we have employed two encryption techniques: one being chaotic encryption and other being DNA encryption. The enormously high sensitivity of chaotic systems to initial conditions is exploited in chaotic encryption. In the proposed work chaotic key sequence created by the logistic map is used for first level encryption. The logistic map is a function that results in a 1D non-periodic chaotic sequence $\{C_i\}$ where the value of C_i ranges from 0 to 1 which is highly random. This can be written as:

$$C_{i+1} = dC_i(1-C_i) \quad (1)$$

The bifurcation parameter (d) ranges from 0 to 4. C_0 is the initial value lying between 0 and 1. The equation can be used to generate the whole sequence of elements $\{C_1, C_2, \ldots C_i, \ldots\}$.The resulting sequence is XORed with watermark bits to get a first level encrypted watermark. Chaotic encryption using a 1D-logistic map is computationally efficient but is associated disadvantage of small key size and hence low security, as such in case of a brute force attack the keys can be compromised. To overcome this disadvantage and enhance the security of the embedded watermark, the already encrypted watermark is re-encrypted using DNA encryption. In computations related to DNA, data is stored in DNA molecules being composed of four nucleotides which are represented as A (Adenine), G (Guanine), T (Thymine), and C (Cytosine). Among these, A and T and C and G are complementary to each other [29] 00 and 11, and 10 and 11 are complementary to each other in binary systems hence they can be used to represent these bases. Among 24 possible combinations, only eight follow complementary rules given by Watson and crick. Table I and Table II show rules for DNA encryption and XOR operation respectively. In this paper, Rule 1 has been used to convert already encrypted watermarked bits into the stream of four nucleotides. The stream obtained is then XORed with the DNA sequence chosen as key to obtain a doubly encrypted watermark. The original watermark and its two-level encrypted versions are shown in Fig. 1. The advantage of using DNA encryption is that both the reference DNA sequence and the complementary rule are necessary for an intruder to discover the secret message being embedded. The probability of which is much less because 163 million DNA sequences are at present available. Both chaotic as well as DNA encryption serve the purpose of providing security to watermark being embedded for copyright protection.

IV. Proposed Framework: DWFCAT

The proposed dual watermarking framework, DWFCAT

TABLE I
DNA Encoding Rules

Rule 1	00-A	01-C	10-G	11-T
Rule 2	00-A	01-G	10-C	11-T
Rule 3	00-C	01-A	10-T	11-G
Rule 4	00-C	01-T	10-A	11-G
Rule 5	00-G	01-A	10-T	11-C
Rule 6	00-G	01-T	10-A	11-C
Rule 7	00-T	01-C	10-G	11-A
Rule 8	00-T	01-G	10-C	11-A

TABLE II
Rules for XOR Operation

XOR	**A**	**T**	**C**	**G**
A	A	T	C	G
T	T	A	G	T
C	C	G	A	T
G	G	C	T	A

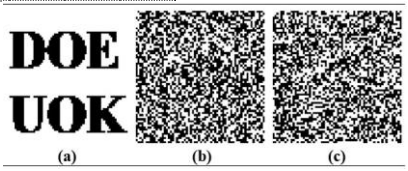

Fig. 1. (a) Original watermark, (b) First stage encryption and (c) Second stage encryption

utilizes a transform domain for embedding a robust watermark and spatial domain for embedding a fragile watermark. We have used the YCbCr color space model to achieve high robustness. Robust watermark has been embedded in the Y channel while the fragile watermark along with overhead bits related to the cover image for tamper localization has been embedded in the Cb channel. The Cr channel is left intact. In the transform domain, DCT has been used because of its energy compaction property. This property of DCT makes the proposed scheme highly robust and imperceptible. The robust watermarking scheme is made more secure by doubly

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3028612, IEEE Transactions on Industrial Informatics

encrypting the watermark using chaotic and DNA encryption before embedding. The high correlation between adjacent pixels has been exploited in the proposed scheme to embed fragile watermark bits. The proposed scheme uses a 4-point neighborhood to forecast the value of a predefined pixel and use that for embedding the fragile watermark bit. The cover image is partitioned into blocks and in each block, we have just embedded one bit to obtain high imperceptibility. Fig. 2 depicts the block diagram of the proposed framework. The Algorithms 1-4 describe the embedding process as well as the process used for extraction for both the watermarks in detail.

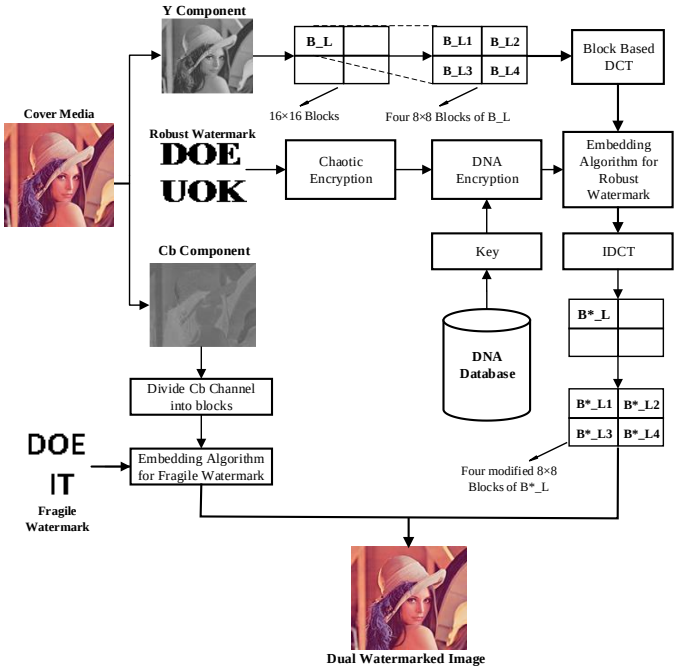

Fig. 2. Block diagram of the proposed secure dual watermarking framework

A. Embedding Algorithms

The proposed algorithm uses the transform domain and spatial domain for embedding a robust watermark and a fragile watermark respectively.

1) Embedding Robust Watermark

The encrypted robust watermark is embedded in the luminance channel of the image. Algorithm 1 enlists the steps used for embedding.

2) Embedding Fragile Watermark

The framework presented in this paper embeds the fragile watermark in the chrominance channel after the robust watermark has been already embedded in the Y channel. The proposed scheme makes use of a 4-point neighborhood to predict the value of a predefined pixel and use that for embedding the fragile watermark bit. Algorithm 2 describes the embedding of a fragile watermark.

Algorithm 1: The process used for embedding the robust watermark

Input: Original Image 'I' and encrypted binary watermark logo

1. Convert the watermark logo into a binary sequence.
2. Convert the RGB cover image (I) into the YCbCr color space and separate the converted image into its constituent channels i.e., Y, Cb Cr. Y channel is selected for embedding the robust watermark.
3. Divide the Y channel into 16×16 non-overlapping blocks. Every block is additionally partitioned into four 8×8 blocks, Bx. Where x = 1, 2, 3, 4.
4. Apply two-dimensional DCT as:
$$D_x = \text{dct2}(B_x) \quad (2)$$
5. Select two blocks out of four blocks Dx in each cycle. Select two mid-frequency coefficients each from a pair of blocks, say Dx1 (m, n) - Dx2 (o, p). Calculate difference as:
$$\psi = D_{x1}(m, n) - D_{x2}(o, p) \quad (3)$$
So, a total of 4 watermark bits are embedded in each 16×16 block.
6. This difference is manipulated as per the encrypted watermark bit so that it occupies one among the four already defined sectors. For watermark bit '0', the difference is adjusted so that it occupies sector 2 (or 4) else the difference is made to lie in sector 1(or 3) whichever is closer to actual difference value. This is achieved as follows:
$$\psi_1 = \begin{cases} \psi \pm \alpha; & for\,sector1 \\ \psi \pm \beta; & for\,sector3 \end{cases} \quad (4)$$
$$\psi_0 = \begin{cases} \psi \pm \delta; & for\,sector2 \\ \psi \pm \lambda; & for\,sector4 \end{cases} \quad (5)$$
The values of 'α', 'β', 'δ' and 'λ' are decided as per the watermark bit, 'Ψ' and neighboring sector. The selected coefficients are modified as per this difference such that difference falls in the designated sector.
7. Inverse DCT of the modified image blocks is taken to get them back in the spatial domain.
8. Modified blocks are combined to get the watermarked Y channel.

Output: Watermarked Y channel

Algorithm 2: Embedding process for fragile watermark

Input: Cb channel of the cover image and fragile watermark

1. Convert the watermark into a binary sequence.
2. Divide the Cb channel into 8×8 non-overlapping blocks.
3. Predict the pixel value of a pre-selected pixel using adjacent 4-point neighbourhood values:
$$P'(x,y) = \frac{P(x+1,y) + P(x-1,y) + P(x,y+1) + P(x,y-1)}{4} \quad (6)$$
where P(i, j) and P'(i, j) are original and predicted value respectively.
4. Then obtain the prediction error by taking the difference between the original pixel value and the one predicted:
$$Pr(x,y) = P(x,y) - P'(x,y) \quad (7)$$
5. Then by expanding, prediction error embeds a watermark bit with each block.
$$Pr'(x,y) = 2*Pr(x,y) + w_i \quad (8)$$
where w_i= 0 or 1.
6. The watermarked pixel values are obtained by summing up predicted values and modified prediction error values as:
$$P''(x,y) = P'(x,y) + Pr'(x,y) \quad (9)$$
7. The pixel values obtained after embedding watermark bits ought to lie between 0 and 255. A location map is formed if the condition is not met. In our scheme, neither overflow nor underflow occurs.
8. Modified blocks are combined to get the watermarked Cb channel.

Output: Watermarked Cb channel

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3028612, IEEE Transactions on Industrial Informatics

For tamper localization, extra information related to cover image is also embedded in the Cb channel in a way that the pixels which are used for embedding fragile watermark remain unchanged. Then watermarked Y channel and Cb channel are concatenated with unmodified Cr channel to obtain a dual watermarked image in YCbCr color space, which is finally converted back to RGB color space.

B. Extraction Algorithms

The original watermarks are not needed at the extraction stage because the proposed framework is blind. The dual watermarked image is initially converted into the YCbCr color space model and among the three channels, Y channel is selected for extracting doubly encrypted robust watermark and the Cb channel is selected for extracting fragile watermark and information related to areas being tampered.

1) Extracting Robust Watermark

The process used for extraction is just the opposite of the one used for embedding and is described as follows:

Algorithm 3: Extraction process of robust watermark

Input: Dual Watermarked image

1. Change the RGB cover image into the YCbCr color space model and separate the converted cover image into the Y, Cb, and Cr channels. The robust watermark is then extracted from the Y channel.
2. Partition the Y channel into 16×16 non-overlapping blocks. Then additionally break each block into four 8×8 blocks.
3. Apply two-dimensional block-level DCT to each 8×8 block to create resultant DCT-transformed blocks.
4. Only the middle-frequency coefficients modified during the embedding process are used for extraction. The actual difference between two pre-defined coefficients decides the bit that was embedded. Bit '0' is extracted If the difference is in sector 2 or sector 4 while bit '1' is extracted if difference lies in sector 1 or sector 3.
5. The original robust watermark is obtained after the decryption of extracted watermark bits.

Output: Binary robust watermark

2) Extracting Fragile Watermark

The extraction procedure used is described as under.

Algorithm 4: Extraction process

Input: Watermarked Cb plane

1. The watermarked Cb channel is selected for extracting the fragile watermark.
2. Split the watermarked Cb channel into 8×8 non-overlap blocks.
3. Predict the pixel value of a pre-selected pixel using adjacent 4-point neighborhood pixel values

$$P\hat{}(x,y) = \frac{Pw(x+1,y) + Pw(x-1,y) + Pw(x,y+1) + Pw(x,y-1)}{4} \quad (10)$$

where Pw(x, y) is the original watermarked pixel.

4. Then the prediction error is obtained by taking the difference between watermarked value and the value predicted

$$Pr\hat{}(x,y) = Pw(x,y) - P\hat{}(x,y) \quad (11)$$

5. Extract watermark bits w_e as

$$w_e = Pr\hat{}(x,y) \bmod 2 \quad (12)$$

Output: Fragile watermark

V. Experimental Results

We have conducted experiments on eight different frequently used color test images, i.e., "Sailboat", "Airplane", "Splash", "Tiffany", "House", "Lena", "Baboon" and "Peppers" which are of size 512×512. The size of the two watermarks used is 64×64. Different test images and watermarks used have been presented shown in Fig.3. The different quality metrics used in the proposed framework include structural similarity index metric (SSIM), bit error rate (BER), peak signal to noise ratio (PSNR) and normalized correlation coefficient (NCC).

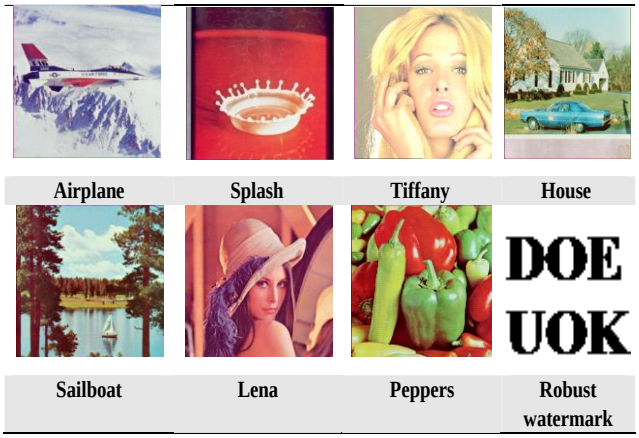

Fig. 3. Various test images and watermarks used

A. Imperceptibility Analysis

The primary requirement of any watermarking system is the imperceptibility. Fig.4 shows the subjective quality of some of the watermarked images along with original images. It is obvious from Fig.4 that the dual watermarked images are of good visual quality. The objective analysis results in terms of peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) have been presented in Table III.

Fig. 4. Watermarked images along with extracted watermarks under no attack

The comparison of average IQA values of the proposed framework with [28] has been given in Table IV. The PSNR values obtained for different dual watermarked images are greater than 41dB demonstrating that the proposed framework is proficient in providing watermarked images of good quality.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3028612, IEEE Transactions on Industrial Informatics

TABLE III
IQA VALUES OBTAINED FOR DUAL WATERMARKED IMAGES

Images	IQA	Robust watermarked	Fragile watermarked	Dual watermarked
Lena	***PSNR***	42.4403	47.7480	41.7021
	SSIM	0.9985	0.9995	0.9981
Pepper	***PSNR***	42.3360	46.0374	41.1219
	SSIM	0.9984	0.9993	0.9979
Sailboat	***PSNR***	41.1678	44.5368	39.7646
	SSIM	0.9953	0.9980	0.9938
Airplane	***PSNR***	41.2703	51.5163	41.2326
	SSIM	0.9784	0.9972	0.9782
Tiffany	***PSNR***	42.7537	46.7723	41.6386
	SSIM	0.9976	0.9990	0.9970
Splash	***PSNR***	43.0753	50.1516	42.7760
	SSIM	0.9968	0.9994	0.9966
House	***PSNR***	41.1235	48.4057	40.6786
	SSIM	0.9931	0.9986	0.9926

TABLE IV
COMPARISON OF AVERAGE IQA VALUES [28]

IQA	PSNR (dB)	SSIM
Robust watermarked [28]	40.85	0.9858
Robust watermarked(proposed)	42.02	0.9940
Fragile watermarked [28]	49.75	0.9968
Fragile watermarked(proposed)	47.88	0.9987
Dual watermarked [28]	40.32	0.9820
Dual watermarked(proposed)	41.27	0.9934

B. Robustness Analysis

In mechanisms for copyright protection, robustness is the most significant apprehension and represents the ability of a watermarking system to resist different attacks. We have subjected the test image "Lena" to various singular and hybrid attacks to assess the robustness of the proposed framework. The attacks performed include "salt and pepper", "Gaussian noise", "JPEG compression", "rotation", "low pass filtering", "darkening", "brightening", "resizing", "cropping", "sharpening" and "histogram equalization". After watermark extraction and decryption, the two most important metrics NCC and BER were computed for assessing the robustness of the proposed technique. Fig. 5 shows the images subjected to various attacks mentioned above and extracted watermarks along with corresponding values of NCC and BER.

Fig.5 shows that irrespective of severe distortion of attacked images, the watermarks extracted are still identifiable and values for NCC and BER are close to 1 and 0 respectively. For highlighting the robustness of the proposed secure scheme, a quantitative comparison of the proposed scheme with some similar schemes has been presented in Table V. Table VI gives the comparison results with Abraham [16] in terms of BER and NCC values for the attacks not present in table IV.

Fig. 5. Extracted robust watermarks along with attacked images.

TABLE VI
COMPARATIVE ANALYSIS OF OUR SCHEME FOR VARIOUS ATTACKS [16]

Attack type	Lena			
	[16]		Proposed	
	BER	NCC	BER	NCC
Salt and pepper (0.01)	0.0391	0.9710	0.1106	0.9198
Speckle (0.01)	0 .1211	0.9129	0.0994	0.9281
Average filter	0.0771	0.9451	0.0850	0.9388
Poisson	0 .1270	0.9085	0.0593	0.9576
Gaussian LPF	0.0010	0.9993	0	1
LSB reset (1 or 2)	0	1	0	1
LSB reset (1-3)	0 .0117	1	0	1
LSB reset (1-4)	0 .1104	0. 9205	0	1
Cropping (25%)	0.2500	0. 7500	0.1296	0.9057
Cropping (50%)	0.5000	0.5000	0.2593	0.8047
Cropping (75%)	0 .7500	0. 2500	0.3145	0.7603
Sharpening	0 .0781	0.9455	0.0513	0.9633
Resize (50%)	0.0518	0. 96330	0	1
JPEG Compression (Q =40)	0.1982	0.8549	0.1240	0.9098
JPEG Compression (Q=50)	0.1543	0. .8873	0.0122	0.9914
JPEG Compression (Q =60)	0.2617	0. 8057	0.0002	0.9998
JPEG Compression (Q=70)	0 .2295	0.8314	0	1
JPEG Compression (Q =80)	0.1875	0. 8648	0	1

Table VI shows that after embedding two watermarks still the average BER and NCC values obtained are better than those presented in [16]. In addition to singular attacks, the scheme has been evaluated for hybrid attacks as well, and results obtained for hybrid attacks have been shown in Fig.6. The proposed scheme provides very good results for hybrid attacks as well, hence making it more suitable for the real-world scenario.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.3028612, IEEE Transactions on Industrial Informatics

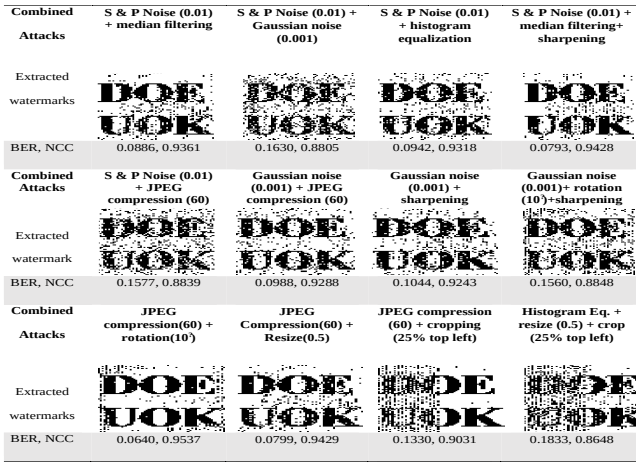

Fig. 6. Extracted robust watermarks along with attacked images after different hybrid attacks

C. *Fragility Analysis of DWFCAT*

The fragile watermarking scheme was developed for authentication and tamper localization of RGB color images. We have assessed the fragility of the proposed scheme to singular attacks such as S & P Noise, Gaussian noise, Median filtering, Histogram equalization, Sharpening, Low pass filtering, and Cropping. The watermarks extracted along with BER and NCC values have been presented in Fig.7.

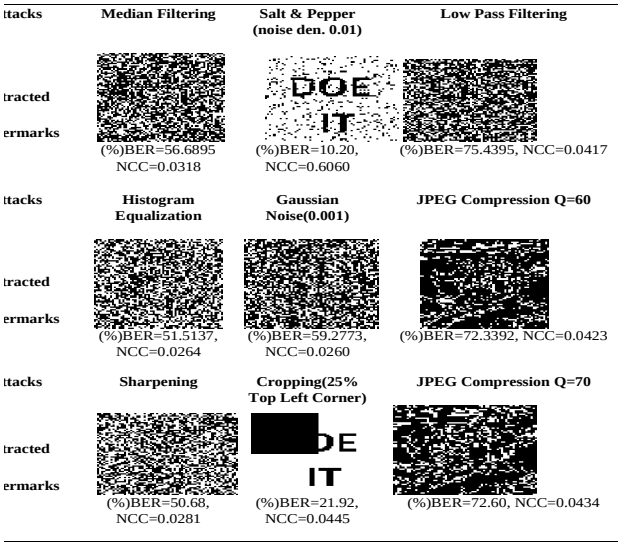

Fig. 7. Extracted Fragile watermarks after various singular attacks

D. *Tamper Localization*

The watermarking system should be able to localize any kind of tampering done to watermarked images by an intruder. The fragile watermark embedded in our scheme is only able to authenticate the color images being transmitted. However, the proposed scheme is blind hence for tamper localization overhead bits have been embedded in the Cb channel in addition to fragile watermark Fig. 8 shows the results obtained after subjecting watermarked images to few forgery attacks. As can be seen from the results obtained, the scheme presented in this paper can accurately locate the areas being tampered.

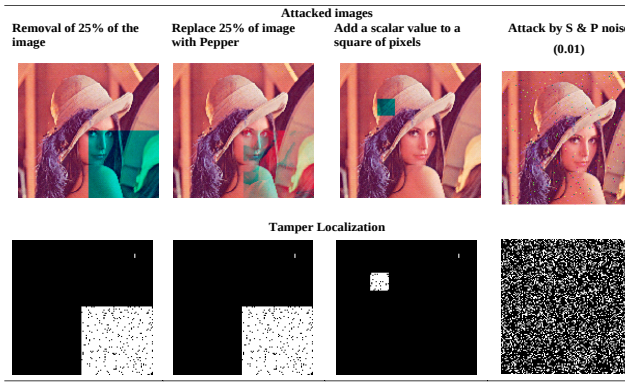

Fig. 8. Extracted fragile watermarks after various singular attacks

E. *Complexity*

The experimental analysis in terms of the execution time of the proposed algorithm has been performed on MATLAB 2017b platform using Windows OS with processor Intel (R) Core™ Duo CPU T5870 @2.00 GHz and results obtained for each module have been shown in Table VII. It is pertinent to mention that various times presented in Table VII are the average times obtained for all the test images at various image resolutions.

TABLE VII
TIMING ANALYSIS FOR EACH MODULE IN SECONDS

Algorithm Used	Image Resolution	Encryption time(s)	Decryption time(s)
Chaotic encryption	1024×1024	0.1920	0.0200
	512×512	0.1716	0.0134
	256×256	0.1560	0.0122
	128×128	0.0156	0.0116
DNA encryption	1024×1024	1.8686	1.6988
	512×512	0.7020	0.4613
	256×256	0.1404	0.1529
	128×128	0.092	0.0738
		Embedding time(s)	Extraction time(s)
Robust Algorithm	1024×1024	7.1984	2.8018
	512×512	2.2776	0.9204
	256×256	0.7442	0.3565
	128×128	0.3766	0.1248
Fragile Algorithm	1024×1024	0.7188	0.22273
	512×512	0.1426	0.0682
	256×256	0.0340	0.0245
	128×128	0.0188	0.0112

VI. A BRIEF DISCUSSION ABOUT RESULTS

DWFCAT presented in this paper has been analyzed for real-time attack scenarios in terms of imperceptibility, robustness, tamper detection, and tamper localization. The results shown in Table III and Table IV show that our security framework provides better quality watermarked images compared to the state-of-the-art. An average PSNR value of above 41dB testifies our claim. The robustness of the proposed scheme to a range of signal processing and geometric attacks has been successfully evaluated. The subjective and objective results presented in Table V, Table VI, and Fig. 5, show the effectiveness of our scheme. The comparison of various parameters of interest in Tables V and VI show better performance of our scheme compared to existing ones. In addition to testing our scheme for singular attacks, we have tested it for simultaneous attacks as well, as reported in Fig. 6. The subjective and objective results prove that our scheme can

withstand simultaneous attacks as well. The robustness parameter of the proposed scheme ensures to share data faithfully even over a network prone to cyber-attacks. Tamper detection and localization are of paramount importance when data is transferred over an open network like in the case of IoT driven distributed systems. Our scheme can detect tampered regions correctly as shown in Fig. 7 and Fig. 8. Our scheme can even detect tamper caused by signal processing or geometric attacks as can be seen from Fig. 7. An average BER of more than 50% validates our claim. Also, our method is capable of localizing the forged area as shown in Fig. 8, which is of immense importance in industrial informatics. A comprehensive timing analysis presented in Table VII shows that our scheme can be used in real-time scenarios when the image resolution is 512×512 or less.

VII. Conclusion

Image authentication and tamper localization are of paramount importance in a PEC based IoT driven industrial environment. A smart environment like industry 4.0 continuously monitors, records, and transmits information about critical events in the industry. This ensures better organizational control and industrial throughput. The data emanating out of critical PEC, nodes need to be secured, and the receiver should be capable of authenticating the content received and localizing the tamper in the received data if any. Besides, certain critical applications require the exact location of nodes sharing the information in an IoT based distributed system. Towards this end, DWFCAT has been proposed for copyright protection (used to distinctly identify the node), authentication and tamper localization of color images, being transmitted over insecure networks in an IIoT system. A doubly encrypted robust watermark has been embedded in the Y channel and a fragile watermark in the Cb channel of YCbCr color space respectively. DWFCAT can authenticate, detect and localize tamper, and exactly distinguish and protect copyrights of the media (images) obtained from sensor nodes without the requirement of original image and watermarks during extraction. The results obtained confirm that the scheme can stand firm against different singular as well as hybrid attacks and acceptably trace the regions being tampered as well. The average PSNR achieved for a payload of 8192 bits is more than 41 dB. The average NCC of robust watermark for singular attacks is more the 0.95 while as for hybrid attacks it is more than 0.90 and watermarks are well recognizable, which proves that DWFCAT can be used for the protection of important and valuable industrial images. In the future, we aim to employ a self-recovery mechanism with the scheme so that it can recover images after the detection of tampered regions.

References

[1] Xu X., Zhang X., Gao H., Xue Y., Qi L., and Dou W., "BeCome: Block-chain-Enabled Computation Offloading for IoT in Mobile Edge Computing," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4187-4195, June 2020.

[2] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: An intelligent trust evaluation scheme in sensor-cloud enabled industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, 2019.

[3] Xu X, Liu Q, Zhang X., Zhang J., Qi L., Dou W., A block-chain-powered crowdsourcing method with privacy preservation in mobile environment, IEEE Transactions on Computational Social Systems 6 (6), 1407-1419-2019.

[4] T. Wang, H. Luo, W. Jia, A. Liu and M. Xie, "MTES: An Intelligent Trust Evaluation Scheme in Sensor-Cloud-Enabled Industrial Internet of Things," *in IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2054-2062, March 2020, doi: 10.1109/TII.2019.2930286.

[5] E. Sisinni, A. Saifullah, H. Song, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14(11), pp. 4724-4734, 2018.

[6] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 3628-3636, 2017.

[7] Y. Xun, J. Liu, N. Kato, Y. Fang and Y. Zhang, "Automobile Driver Fingerprinting: A New Machine Learning Based Authentication Scheme," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1417-1426, Feb. 2020, doi: 10.1109/TII.2019.2946626.

[8] C. W. Chen, "Internet of Video Things: Next Generation IoT with Visual Sensors," in IEEE Internet of Things Journal, June 2020, doi: 10.1109/JIOT.2020.3005727.

[9] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang and S. W. Baik, "Secure Surveillance Framework for IoT Systems Using Probabilistic Image Encryption," in IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3679-3689, Aug. 2018, doi: 10.1109/TII.2018.2791944.

[10] Domingo-F, Josep, O, Jordi R, and David S. "Privacy-preserving cloud computing on sensitive data: A survey of methods, products, and challenges." Computer Communications 140 (2019): 38-60.

[11] Y. Shi, W. Wei, F. Zhang, X. Luo, Z. He and H. Fan, "SDSRS: A Novel White-Box Cryptography Scheme for Securing Embedded Devices in IIoT," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1602-1616, March 2020, doi: 10.1109/TII.2019.2929431.

[12] Gutub, Adnan, Nouf Al-Juaid, and Esam Khan. "Counting-based secret sharing technique for multimedia applications." *Multimedia Tools and Applications* 78, no. 5 (2019): 5591-5619.

[13] Hathaliya, Jigna J., and Sudeep T. "An exhaustive survey on security and privacy issues in Healthcare 4.0." Computer Communications 153,311-335 (2020).

[14] Jiang, D. "The construction of smart city information system based on the Internet of Things and cloud computing." Computer Communications 150 (2020): 158-166.

[15] Senthilkumar M., and Gautam S. "An efficient public key secure scheme for cloud and IoT security." Computer Communications 150 (2020): 634-643.

[16] Abraham, Jobin, and Varghese P. "An imperceptible spatial domain color image watermarking scheme." Journal of King Saud University-Computer and Information Sciences 31, no. 1 (2019): 125-133.

[17] Chang, CC, Chen K, Lee C, and Liu L. "A secure fragile watermarking scheme based on chaos-and-hamming code." Journal of Systems and Software 84, no. 9 (2011): 1462-1470.

[18] Zhang, Xinpeng, and Shuozhong W. "Fragile watermarking with error-free restoration capability." IEEE Transactions on Multimedia 10, no. 8 (2008): 1490-1499.

[19] Zhang, Jiale, Bing Chen, Yanchao Zhao, Xiang Cheng, and Feng Hu. "Data security and privacy-preserving in edge computing paradigm: Survey and open issues." *IEEE Access* 6 (2018): 18209-18237.

[20] Xiaoying Q, ZhiguoD , Xuan S, "Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks" IEEE Access. Digital Object Identifier 10.1109/ACCESS.2019.2956480.

[21] Feng, Liu P., Liang B., and Peng C. "A DWT-DCT based blind watermarking algorithm for copyright protection." In 2010 3rd International Conference on Computer Science and Information Technology, vol. 7, pp. 455-458. IEEE, 2010.

[22] Kang, Xiangui, Jiwu Huang, Yun Q. Shi, and Yan Lin. "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression." IEEE transactions on circuits and systems for video technology 13, no. 8 (2003): 776-786.

[23] P.-Y. Lin, J.-S. Lee, and C.-C. Chang, "Dual digital watermarking for Internet media based on hybrid strategies," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 8, pp. 1169–1177, Aug. 2009.

[24] Shi, Hui, Ming-chu Li, Cheng Guo, and Ru Tan. "A region-adaptive semi-fragile dual watermarking scheme." Multimedia Tools and Applications 75, no. 1 (2016): 465-495.

[25] S Roy, A K Pal, “A blind DCT based color watermarking algorithm for embedding multiple watermarks.” Int. J. Electron. Commun. (AEÜ) 72 (2017) 149–161.

[26] Lusson, Frédéric, Karen Bailey, Mark Leeney, and Kevin Curran. "A novel approach to digital watermarking, exploiting colour spaces." *Signal Processing* 93, no. 5 (2013): 1268-1294.

[27] Su, Q., Yugang N. Hailin Z., and XianxiL.. "A blind dual color images watermarking based on singular value decomposition." Applied Mathematics and Computation 219, no. 16 (2013): 8455-8466.

[28] Liu, X., Lin C., and Yuan S. "Blind dual watermarking for color images’ authentication and copyright protection." IEEE Transactions on Circuits and Systems for Video Technology 28, no. 5 (2016): 1047-1055.

[29] Liu, Hongjun, and Xingyuan Wang. "Image encryption using DNA complementary rule and chaotic maps." Applied Soft Computing 12, no. 5 (2012): 1457-1466.