Research Article

A publicly verifiable watermarking scheme based on quantum chaos and DWT–DCT

Gaurav Sharma[1] · Rashmi Chawla[1] · Shailender Gupta[1] · Shirin Dora[2]

Received: 23 July 2019 / Accepted: 22 November 2019 / Published online: 27 November 2019

Abstract

One of the problems faced by the internet consumer in today's data age is protection of digital rights or ownership of intellectual property (IP) due to multi-fold sharing of data without consent. As a result, anti-piracy, a domain of robust IP protection has become a cardinal subject of research in system design. In this regards, watermarking has emerged as one of the best protection of authorship since it provides protection against tampering without any perceivable change in the multimedia content. This research paper focuses on developing a robust watermarking scheme. The proposed approach employs quantum chaos based encryption algorithm having low time complexity and optimized entropy values thereby reducing the chances of statistical attacks. In addition, SHA-3 is used for creating the digest as it affords easier hardware implementation and high security. DCT–DWT hybrid model is used for embedding watermark to further enhance robustness and RC4 with quantum chaos coupled with neighbouring coupled map lattice sequence as key for allocating random position to watermark pixels. The scheme provides improved results against existing noise based geometric attacks, universal image quality index and visual assessments in comparison to other mechanism in literature.

Keywords Peak signal to noise ratio · Universal image quality index · Structural similarity

1 Introduction

The network connectivity has increased manifold in the past decade and market is estimated to grow to 2898.9 Million USD by 2020 [1]. This increase makes it easier to share multimedia information efficiently at high speed. However, the downside of the same is frequent violations of intellectual property (IP) rights owing to unauthorized use of the data mainly in terms of reproduction and distribution resulting in a huge financial loss for IP owners [2]. IP rights play the crucial role of ensuring that proper incentives are served to the IP holders. Infringement of IP rights is known as piracy in which the work is distributed, reproduced, used directly or derivative without copyright holder's permission.

Watermarking is one amid various applied techniques for ensuing unauthorized access, intercepting illegal replication, establishing ownership rights, and facilitating content authentication. It involves embedding special elements within the content in order to authenticate the ownership of the IP [3, 4]. Numerous mechanisms for IP protection have been proposed and the search still goes on since attackers continuously tries to attack the watermark [5–8] with the aim to break its security feature. Some of the desirable features of a good watermarking technique are (1) owner protection (2) highly robust (3) versatile (4) strongly imperceptible (5) potential to identify owner/developer. Keeping these aspects in mind myriad researchers in past have proposed different watermarking techniques [9–12]. Some of the existing algorithms [13–17]

✉ Rashmi Chawla, rashmichawlaymca@gmail.com; Gaurav Sharma, sharma.grv69@gmail.com; Shailender Gupta, shailender81@gmail.com; Shirin Dora, shirin.dora@gmail.com | [1]J.C. Bose University of Science and Technology, YMCA, Faridabad, Haryana, India. [2]University of Ulster, Londonderry, Northern Ireland.

preserve the multimedia content but are vulnerable to geometric attacks. This paper identifies the shortcoming of the watermarking algorithms available in literature and concedes an enhanced and robust watermarking algorithm.

The quantum chaos based encryption algorithm owing to low time complexity and optimized entropy values is employed to curtail statistical attacks. Withal to this highly secured and easily applicable SHA-3 is used for creating the digest. To work on robustness this research work proposes DCT–DWT hybrid model for embedding watermark and RC4 with quantum chaos for randomness enhancement. To work efficiently on allocating position to watermark pixels RC4 is coupled with NCML sequence for key designing. The proposed work promises outdo results against existing noise based geometric attacks viz. Gaussian/salt-pepper and UIQI.

The next section gives a brief on past literature work in detail and problem definition. The details of the proposed algorithm are given in Sect. 3. Section 4 gives the simulation setup parameters employed contemplating robustness and efficiency of the proposed mechanism. Comparison results of the proposed scheme with the latest technique available in literature are manifested in the following section followed by conclusion and references.

2 Literature survey and problem identification

The past research focusing on watermarking techniques analogous to the proposed mechanism is exhibited in Table 1.

The aforementioned past research shows need for an improved robust watermarking technique still persists to match pace with the fast heading technology. This research work aims resolving the past setbacks with following objectives.

Objectives	Ownership Protection: This is the utmost requirement of any watermarking technique. It must be extremely easy for the owner to verify its ownership while for impostor it must be extremely difficult.
	Robustness: The watermarking algorithm must be robust against geometric attacks. For that it should use latest frequency domain techniques.
	Integrity of Signature: To maintain integrity of the signature, the watermarking scheme must use latest hashing algorithms available in literature.
	Embedding Signature in Random Positions: The watermark should be appended in random positions. Thus, latest algorithms to search random positions for inserting signature should be employed.

The next section deals with proposed watermarking scheme in detail.

3 The proposed watermarking scheme

The proposed research illustrated in Fig. 1 illustrates making of a robust watermark and mechanism to append it in a cover media to protect the ownership of the multimedia content. The salient features of the proposed algorithm are:

- Employment of DWT–DCT that helps in improving robustness of the proposed scheme in comparison to Zhang et al. scheme.
- The process uses quantum chaos mechanism to improve randomness in data embedding process making it extremely difficult for the other persons to find out the position of watermark.
- Quantum cryptographic algorithm is used which has very high execution speed and brute force search time.
- Employment of latest hashing technique also improves the integrity process.

The proposal is divided into three inherent parts (1) watermark computation (2) watermark embedding (3) watermark verification

3.1 Watermark computation

In this stage, first of all random numbers are generated using quantum logistic map equations provided in Goggin et al. [16] and Akhavan et al. [19].

3.1.1 Quantum logistic map equation

$$
\begin{aligned}
X(n+1) &= r \times \left(X(n) - |X(n)|^2\right) - r \times Y(n)\\
Y(n+1) &= -Y(n) \times e^{-2\beta} + e^{-\beta} \times r \times \left[(2 - X(n) - X^*(n))\right.\\
&\qquad \left. \times Y(n) - X(n) \times Z^*(n) - X^*(n) \times Z(n)\right]\\
Z(n+1) &= -Z(n) \times e^{-2\beta} + e^{-\beta} \times r \times \left[2 \times (1 - X^*(n))\right.\\
&\qquad \left. \times Z(n) - 2 \times X(n) \times Y(n) - X(n)\right]
\end{aligned}
$$

Where the initial key parameters are:

1. ***X*(0), *Y*(0), *Z*(0),**
2. $\boldsymbol{X}^*(0)$, $\boldsymbol{Z}^*(0)$ {complex conjugates of X and Z},
3. $\boldsymbol{r}$ (also known as control parameter),
4. β (dissipation parameter).

This quantum logistic map generated string is independently coupled with NCML.

Equation set for coupling:

Table 1 Literature survey

S. No.	Authors	Work done	Pros/cons
1	Lach et al. [4]	Used small watermarks instead of single one with the aim to increase robustness It uses subset of watermark for verification	Leakage of watermark positions after public verification is susceptible to tampering. Hence, this technique may pose a serious threat to ownership of the message
2	Qu et al. [5]	Two level verification process Separate watermark intended for public verification A public one-way hash function on the header is applied	After public verification step is applied, the location of watermark embedding positions is exposed. Again, it's also a threat to ownership Tampering is possible for public watermark showing the technique is not robust The integrity of the header can be improved using latest algorithms available in literature
3	Qu et al. [6]	Proposes public–private watermark Public watermark verification is done through exposing the encoding scheme	It's a compromise with the message authenticity of the watermark
4	Saha et al. [7]	Zero-knowledge-based FPGA digital signature Uses proof of knowledge in cryptography and zero knowledge about the system	Fraudulent IP buyers can pose security threat Robustness is not good
5	Zhang et al. [8]	Based on zero-overhead and can easily resist the removal of watermarks	Exposed embedding positions hence, vulnerable to message ownership Robustness is not good
6	Zhang et al. [18]	Time stamping and zero-knowledge interaction based on chaos theory Pseudorandom number generator for deciding embedding position Watermarking is embedded based on spread spectrum watermarking IP rights protection is the best up till now	The use of DCT makes the proposal robust but can be further improved by using hybrid approach (DCT coupled with DWT) The entropy values for pseudorandom process can be improved further by employing quantum chaos with NCML maps Improvements to hash function, cryptographic algorithm employed can be done
10	Han Fang et al. [9]	Investigation of relationship between positions and modification magnitude is proposed to increase robustness Gabor filter is used to detect texture direction The texture direction is further embedded with one watermark based on coefficient of texture direction	A direction-coefficient mapping is done based on position and magnitude relationship The texture block direction features is used for increasing robustness of the watermark image
11	Wang et al. [10]	To resist geometric attacks an optimal synchronization correction-based digital image watermarking method is proposed Utilizing the compact image feature, the least squares support vector regression (LS-SVR) synchronization correction is performed to estimate the geometric distortions parameters	This approach consists of watermark embedding, synchronization correction and watermark extraction
12	Sadeghi et al. [11]	The host signal projected samples in random space are considered to enhance watermarking robustness Further quantization of the ratio of the two projections is done to preserve the watermark imperceptibility	The maximum likelihood detector on the basis of error probability is derived and analyzed in terms of watermarking noise ratio
13	Najafi et al. [12]	The contoured trans-form with singular value decomposition (SVD) and sharp frequency localized is proposed as a secure and robust image watermarking method	The proposal exhibits good imperceptibility and robustness for the image processing applications
14.	Mohanty et al. [19]	Linear feedback shift registers (LFSR) is used to add watermark	PSNR low values exhibit low robustness and threat to the Watermarked images Requires prior information hence not good as Zhang et al.

Table 1 (continued)

S. No.	Authors	Work done	Pros/cons
15.	Chang et al. [20]	Cryptographic hash function is employed for data authentication	The research work missed unique binding parameter resulting in tampering execution posing threat to data Robustness is not good
16.	Chroni et al. [21]	Codec algorithm is proposed for uploading watermarking in 2D images in the spatial domain on the web under (IP) protection Discrete Fourier Transform (DFT) Is proposed for robustness Experimental evaluation of proposed algorithm employing different images under JPEG compression is done	The partial modification in an image enables self-inverting permutations for an efficient watermarking technique Robustness parameter can be further improved by employing other frequency domain transforms coupled with wavelets domain technique
17.	Sharma et al. [22]	Uses quantum encryption scheme Watermark image quality is too good Focus on image perceptual quality not robustness	Robustness against JPEG compression, salt and paper noise attacks is poor To improve robustness frequency domain techniques should be used

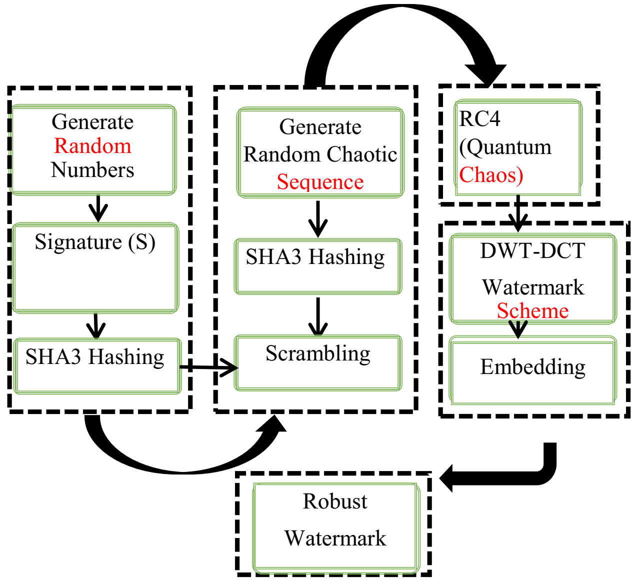


Fig. 1 Block description of the proposed watermarking algorithm

$$X_n^{coupled}(k) = (1-e)\times\left(X_n(k+1)\right) + (e)\times Y_n(k+1)$$
$$Y_n^{coupled}(k) = (1-e)\times\left(Y_n(k+1)\right) + (e)\times Z_n(k+1)$$
$$Z_n^{coupled}(k) = (1-e)\times\left(Z_n(k+1)\right) + (e)\times X_n(k+1)$$

where X_n, Y_n, Z_n are the random numbers generated using quantum chaos scheme $X_n^{coupled}, Y_n^{coupled}, Z_n^{coupled}$ are the sequences obtained using NCML equations

This random sequence is used for encrypting the Signature (S) using a key whose value is given in set up parameters. Finally the encrypted signature is hashed using latest SHA-3 [23] algorithm to obtain encrypted digest. This digest is scrambled (XORed) with another digest obtained after applying SHA-3 on random chaotic sequences to obtain the watermark. The watermark is appended in random positions which are generated using RC4. The input key to RC4 is provided using quantum logistic equations mentioned above. The next section shows embedding of this watermark in the multimedia content.

3.2 Watermark embedding

The process of embedding is done using hybrid model i.e. combining DCT with Wavelet transform. The steps towards implementation of DWT–DCT hybrid embedding are as follows:

Step 1 As suggested from the name of hybridization, the first transformation will be the Two-dimensional

Discrete Wavelet Transform (DWT) applied on the full cover image

Step 2 The result comprises of 4 matrices, approximation coefficients matrix cA (or LL in the diagram) and details coefficients matrices cH, cV, and cD(horizontal (LH), vertical (HL), and diagonal (HH), respectively)

Step 3 In DWT based embedding techniques amongst these matrices the horizontal and vertical matrices are chosen for embedding purposes. Thus, choosing either HL or LH matrix and then applying two-dimensional discrete cosine transforms on it; we get a DWT–DCT block for the purpose of data embedding. The embedding positions are generated RC4

Step 4 The reverse procedure is followed for getting the modified cover image or data embedded cover image.

Pictorially, the technique can be summed up as follows (see Fig. 2).

The advantages of using this hybridization can be seen in the result section ahead where geometric attacks are compared on Standalone DCT and hybridized form.

3.3 Watermark verification

The proposed paper uses same technique as provided by author Zhang et al. [18]. Author derived its basis from the inspiring contributions in literature [21, 24, 25]. The role of chaotic sequence generation in the same is inexplicable. This process is further enhanced by employing quantum logistic map coupled with NCML so as to enhance the robustness [16] nature and the subsequent security of the scheme [26–28].

4 Experimental setup

4.1 Set up parameters

The setup parameters are illustrated in Fig. 3 and enlisted in Table 2.

4.2 Snapshots

The snapshots of results along with the histogram are shown in Table 3. The histogram of both the techniques (1) base paper—Zhang et al. [18] (2) proposed technique, show same result on ownership protection. The histogram indicates that watermarking scheme performs quite well in hiding the data in the original image. Same is the case for Zhang et al. scheme therefore no visual inference can be drawn from the histogram results. The performance metrics in terms of robustness and other parameters is covered in next section.

5 Results

To check the efficacy of the proposed scheme, it is compared with one of the robust technique in literature provided by Zhang and Liu [18]. In addition; it is also compared with Ref. [22] which takes image perceptual quality as the performance metric. The next subsections give

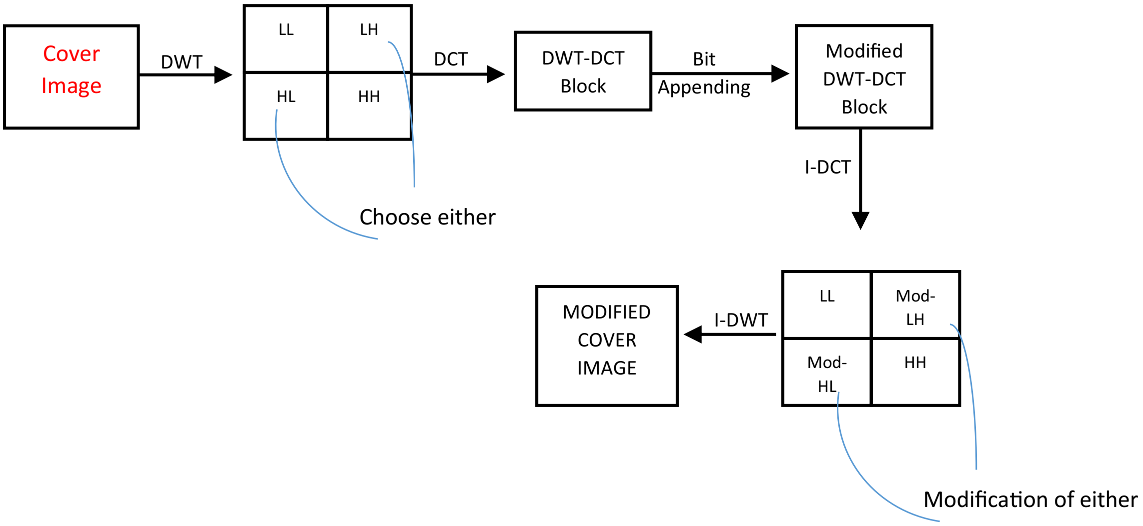


Fig. 2 Embedding DWT–DCT block diagram

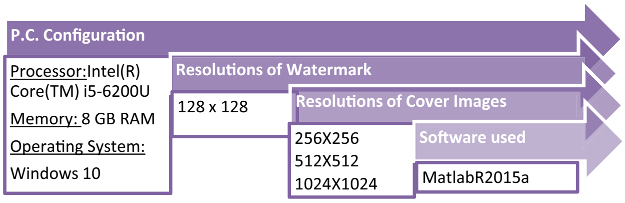


Fig. 3 Set up parameters used in computation

the detail of improvements obtained in performance parameters:

5.1 Ownership protection

5.1.1 Impact on correlation coefficient

To protect the ownership of the multimedia content, it should perfectly match with the original data. Therefore, correlation is calculated between original and watermarked image. The following points can be inferred:

- Correlation obtained in proposed mechanism maintains consistent value for all image sizes unlike the base algorithm (Zhang et al.) where it increases with image size.
- Table 4 depicts that the correlation between cover image and watermarked image is higher in proposed algorithm as compared to the base algorithm. A better correlation signifies much more visual similarity between cover and watermarked image, which in turn shows that higher level of imperceptibility is achieved in proposed technique.

5.1.2 Impact on PSNR

The PSNR is basically the ratio of maximum power of signal to power of noise [25, 26, 29, 30]. More is its value better is the ownership of the document.

- Referring to Table 5, it can be clearly observed that PSNR values are comparatively higher in proposed technique for all image sizes. The better values of PSNR between cover and watermarked image indicate that image quality is better retained in the proposed version.
- Also, PSNR increases as the image size increases.

5.1.3 Impact on SSIM (structural similarity)

- Figure 4 shows that SSIM index is greater for proposed algorithm in each case i.e. for every image size. The numeric data is represented in Table 6.
- Also, SSIM Index of proposed algorithm is maintaining a consistent value unlike that of reference which rises with the increase in image size.

5.2 Robustness analysis

5.2.1 Impact on correlation coefficient

The watermark verification system can be manipulated if one includes some noise like pattern or its own watermark at different places overshadowing the original watermark. Thus, more than any of the other geometric attacks, such as affine transformations or cropping attacks, the analysis of recovered watermark after noise is added to the watermarked image seems necessary.

Table 2 Set up parameters

Parameter values for chaos based encryption algorithm [12, 13]	
a = 1.77; b = 1.67; c = −0.85; d = 2.1; X(0) = 0.6; Y(0) = 0.4	
Parameter values for Akhshani et al. [13] (quantum chaos based encryption)	
r = 3.99; b = 6; x(n) = 0.4523444336; y(n) = 0.003453324562; z(n) = 0.001324523564; $x^{*}(n)$ = x(n); $z^{*}(n)$ = z(n)d	
Parameter values for logistic map	
For key 1:	For key 2:
x(0) = 0.2; μ = 3.999	x(0) = 0.199; μ = 3.999
Parameter values for quantum logistic map and NCML	
For key 1:	For key 2:
r = 3.99; b = 4.489; x(n) = 0.463442265; y(n) = 0.004532285; z(n) = 0.002136285; $x^{*}(n)$ = 0.00186; $z^{*}(n)$ = 0.00398	r = 3.99; b = 4.489; x(n) = 0.473442265; y(n) = 0.004632285; z(n) = 0.002236285; $x^{*}(n)$ = 0.00196; $z^{*}(n)$ = 0.00308
For NCML:	For NCML:
e = 0.001	e = 0.001

Table 3 Snapshots and histogram of results

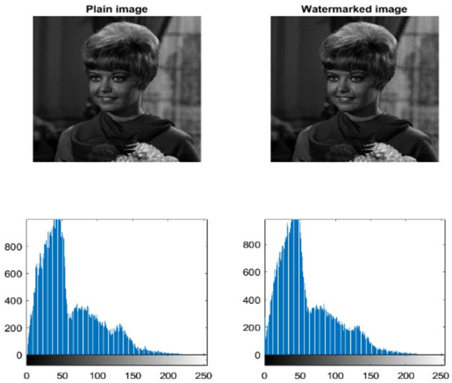
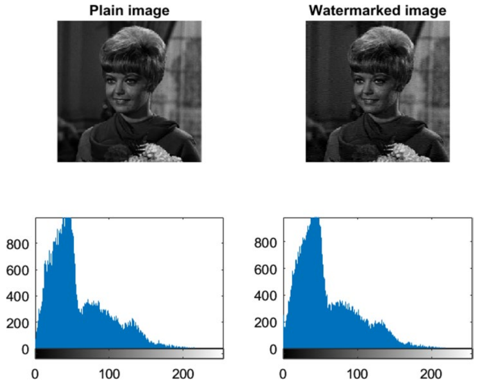
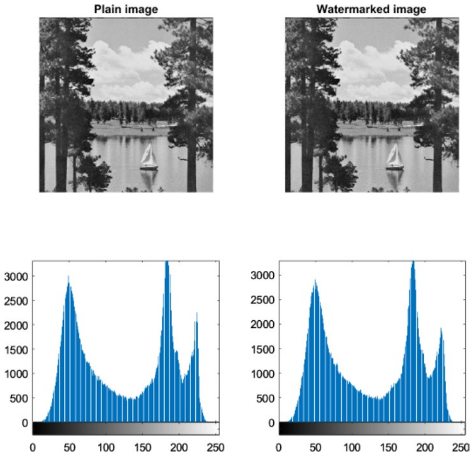
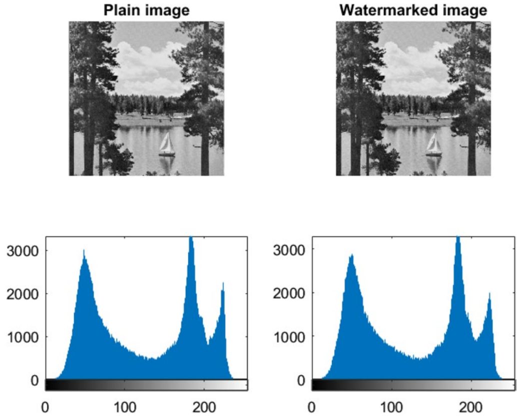
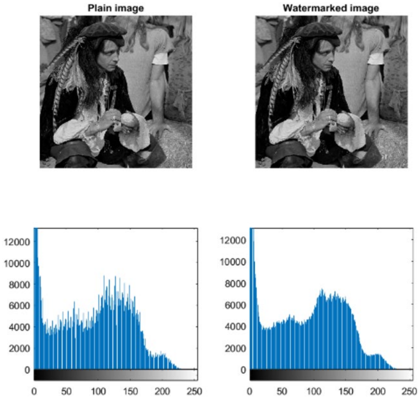
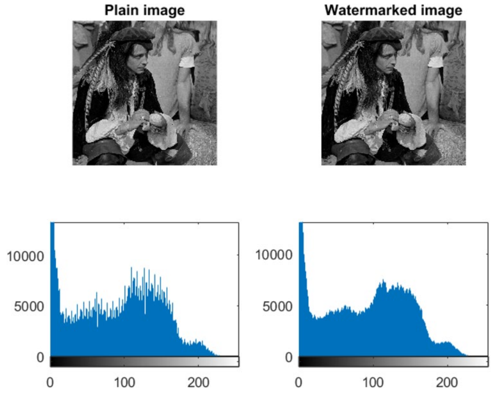
Image source	The images are taken from USC-SIPI image database. The link for the same is: https://sipi.usc.edu/database/database.php?volume=misc&image=23#top	
Image size	Base paper	Proposed technique
	Image and its histogram	Image and its histogram
256×256		
512×512		
1024×1024		

Table 4 Correlation coefficient versus image size

Image size	Zhang et al. [18]	Proposed
256×256	0.994872991±0.03%	0.99486363±0.04%
512×512	0.999525412±0.02%	0.999525843±0.03%
1024×1024	0.999849534±0.03%	0.999841009±0.01%

Table 5 PSNR versus image size

Image size	Zhang et al.	Proposed
256×256	35.9964797±0.04%	36.00377472±0.03%
512×512	42.02217023±0.03%	42.01826351±0.02%
1024×1024	47.848661±0.02%	48.08797848±0.04%

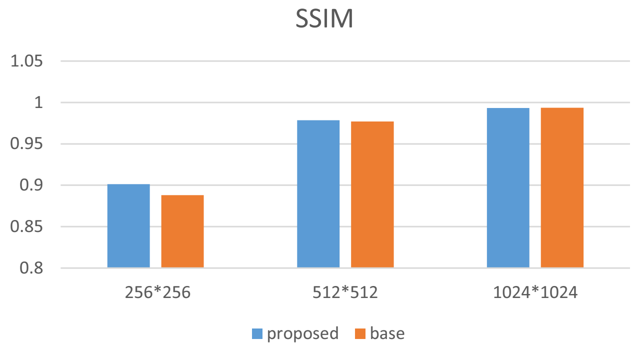


Fig. 4 SSIM versus image size

Table 6 SSIM versus image size

Image size	Zhang et al.	Proposed
256 × 256	0.888184594 ± 0.03%	0.890169377 ± 0.02%
512 × 512	0.976918735 ± 0.01	0.977372302 ± 0.03%
1024 × 1024	0.99359509 ± 0.02%	0.993468966 ± 0.03%

To check the robustness of the proposed algorithm against attacks, correlation is calculated after applying geometric attacks on the watermarked image. It was found that in most of the cases; proposed algorithm results into higher correlation indicating that it is more robust than the base algorithm in terms of resistance against geometric attacks (see Figs. 5, 6).

5.2.2 Impact of JPEG compression

To find the impact on JPEG compression, Normalized Correlation Coefficient (NCC) is calculated between the original and water mark extracted for different Quality Factor (QF). It is found that the proposed technique has an edge over the Zhang scheme. At Quality factor 1 meaning no compression is there, the values of NCC for both the techniques are same while for QF = 0.75, the value of NCC is more for proposed algorithm (illustrated in Table 7) due to employment of Hybrid DCT–DWT approach.

5.3 Integrity of signature

The proposed algorithm uses SHA-3 in contrast to SHA-2 used by Zhang et al. Though, both have nearly same efficiency in terms of number of bits change when one bit is changed as can be seen from the Table 8 but SHA-2 is susceptible to length extension attacks. Also, its hardware implementation is easy that's why SHA-3 is used in our proposed algorithm.

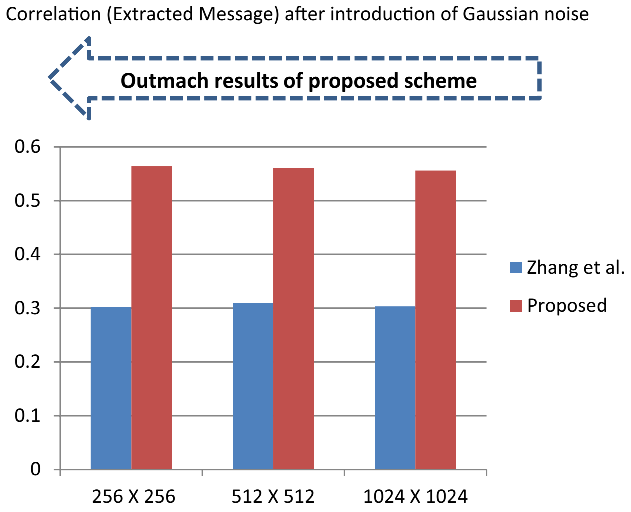


Fig. 5 Correlation (after geometric attack): Gaussian noise

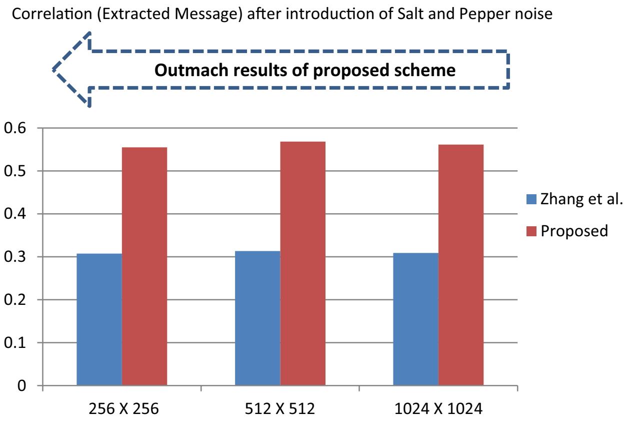


Fig. 6 Correlation (after geometric attack) versus image size

Table 7 Impact of JPEG compression

LEVEL(QF)	Base paper	Proposed
45	0.9957 ± 0.03%	0.9964 ± 0.03%
50	0.9961 ± 0.02%	0.9968 ± 0.02%
55	0.9965 ± 0.02%	0.9971 ± 0.04%
75	0.9981 ± 0.03%	0.9984 ± 0.02%
100	1 ± 0%	1 ± 0%

5.4 Embedding signature in random positions

To find the embedding positions for watermark embedding, the proposed scheme uses RC4 in which input key is generated using quantum chaos scheme instead of chaos method making the generation of random position

Table 8 Comparison of SHA-2 and SHA-3

	Hex output of data 1 = [1 1 1 1 1 1 1 1]	Hexadecimal output of data 2 = [0 1 1 1 1 1 1 1]	Number of bits changed	Length extension attacks
SHA-2	bc3c1cf23193978c80453a4b6c722f5b3cd2783b76b4a417bd2e002d854a4f7a0929988844476642d9fecc2ab86f496363cbe79df4a8abb83570f02f9d0abc12	e8a7205d0112e64f5a4ce1669cad05677f1eb1e5c7f58ff5dffd0ee57735126378f2f40e94fa59c296b3ce9feb1e3c539201284ab4877c2b03f3ef2849007d6b	259	Susceptible
SHA-3	A6F098ADF45424539EB214272E0436894BB6FE3F22F5BF45725E1D4F37313A9547415CA108EA84664995D9CCD3983DC21806765FB8E20D6B686CE51EE6583EC8	D75DAF2BA6283A1FB38AAFEC28D486D60638871030AB17937B82FC83AD843497C5AD238F9779104FF973BBBEE970D4E277AB759A6C28CB17A65E4824E583CAF4	256	Not Susceptible

Table 9 Comparison table metric of the proposed scheme

Image Size (256 × 256)	Zhang et al. [18]	Gaurav et al. [22]	Proposed
Geometric attack	0.3122	0.3454	0.5551
Noise attacks	0.3123	0.2973	0.5632
JPEG compression attack QF = 0.75	0.9981	0.9132	0.9984

more random. Also RC4 is coupled with NCML for further enhancement of randomness.

5.5 Comparison results of proposed scheme

The proposed scheme is compared with Zhang et al. [18] and Gaurav et al. [22] from past literature. Clearly, it indicates from Table 9 that the proposed scheme is best in terms of robustness in comparison to both since it employs DCT–DWT watermarking scheme whereas Gaurav et al. uses spatial domain watermarking technique hence not robust but at the same time gives good picture quality. Also, DCT–DWT is more robust then stand-alone technique such as DCT and DWT, therefore the, the performance metrics lies in the middle of the both.

6 Conclusion

The proposed watermarking scheme outperform Zhang et al. proposal available in literature in terms of all the objectives mentioned above. This proposed scheme is a novel approach for investigating robust watermarking in protection for IP cores. This approach is competent to investigate a low embedding watermark that accounts for satisfactory user specify constraints of randomness. The watermark generated through the proposed approach is based on a DWT–DCT coding scheme with RC4results in robust and secured outcome. The proposal is better in handling the effect of any noise-based geometric attacks (Gaussian and salt-pepper Noise).Besides, robustness watermark generated by this approach, the scheme contents the strong proof of authorship, imperceptibility, resiliency and integrity. The simulation results have confirmed that the proposed approach outmatches

Table 10 Comparative analysis of proposed scheme with past research

Performance Parameters	Zhang et al.	Proposed scheme	Gaurav et al.	Remarks
Ownership Protection	Good	Better	Better	Overlooking the traditional quantitative analysis of PSNR, which comes out to be somewhat better, the modern image enhancement performance parameters of UIQI and SSIM comes out to be great for smaller sized data. Thus ownership is preserved
Robustness	Good	Best	Better	Employment of DWT coupled with DCT helps in attaining better robustness as can be seen from the results also
Integrity of the signature	Somewhat better	Good	Good	The result shows that SHA-3 has almost similar results for one bit is changed but when length extension attack is considered, SHA-3 outperforms its counterpart
Randomness of embedding positions	Good	Better	Better	Employment of quantum chaos as key generation improves randomness of RC4
Perceptual quality	Good	Best	Better	

the recent work in robustness. The concluding points along-with their reasons are thus, enlisted in Table 10.

Apart, from all the advantages one drawback of the proposed scheme is its time complexity, which is on the higher side in comparison to the Zhang et al. scheme due to usage of SHA-3, and DWT–DCT hybrid process. Also, the perceptual quality is also not good when compared to Gaurav et al. scheme due to employment of spatial domain technique for watermark embedding. Therefore, a scheme which has best picture quality after watermark embedding and robustness may be thought of in nearby future.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Markets and markets (2018), https://www.prnewswire.com/news-releases/digital-rights-management-market-worth-28989-million-usd-by-2020-536104821, Accessed 21 Feb 2018
2. Podilchuk CI, Delp EJ (2001) Digital watermarking: algorithms and applications. IEEE Signal Process Mag 18(4):33–46
3. Cox I, Miller M, Bloom J, Fridrich J, Kalker T, Miller M (2007) Digital watermarking and steganography. Morgan Kaufmann, Burlington
4. Lach J, Mangione-Smith WH, Potkonjak M (1999) Robust FPGA intellectual property protection through multiple small watermarks. In: Proceedings of the 36th annual ACM/IEEE design automation conference, ACM, pp 831–836
5. Qu G (2001) Keyless public watermarking for intellectual property authentication. In: International workshop on information hiding, Springer, Berlin, pp. 96–111
6. Qu G (2002) Publicly detectable watermarking for intellectual property authentication in VLSI design. IEEE Trans Comput Aided Des Integr Circuits Syst 21:1363–1368
7. Saha D, Sur-Kolay S (2012) Secure public verification of IP marks in FPGA design through a zero-knowledge protocol. IEEE Trans Very Large Scale Integr (VLSI) Syst 20(10):1749–1757
8. Zhang J, Lin Y, Wu Q, Che W (2012) Watermarking FPGA Bitfile for intellectual property protection. Radioengineering 21(2):764–771
9. Fang H et al (2018) A robust image watermarking scheme in DCT domain based on adaptive texture direction quantization. Multimed Tools Appl 78(22):8075–8089
10. Wang XY et al (2019) Synchronization correction-based robust digital image watermarking approach using Bessel K-form PDF. Pattern Anal Appl. https://doi.org/10.1007/s10044-019-00828-w
11. Sadeghi M et al (2019) Blind Gain invariant image watermarking using random projection approach. Signal Process. https://doi.org/10.1016/j.sigpro.2019.05.026
12. Najafi E et al (2018) Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform. J Inf Secur Appl 44:144–156. https://doi.org/10.1016/j.jisa.2018.12.002
13. Hanchinamani G, Kulkarni L (2015) An efficient image encryption scheme based on a Peter De Jong chaotic map and a RC4 stream cipher. 3D Res 6(3):30
14. Secure Hash Standard (SHS), FIPS 180-4, http://dx.doi.org/10.6028/NIST.FIPS.180-4, 2015
15. Schneier B (1995) Chapter 17—Other stream ciphers and real random-sequence generators. In: Applied cryptography: protocols, algorithms, and source code in C (2nd ed.), Wiley, Hoboken, ISBN: 978-0471117094
16. Goggin ME, Sundaram B, Milonni PW (1990) Quantum logistic map. Phys Rev A 41(10):5705–5708. https://doi.org/10.1103/physreva.41.5705
17. Tuncer T et al (2018) Quantum-dot cellular automata based fragile watermarking method for tamper detection using Chaos. Int J Inf Technol Comput Sci 10(12):27–32
18. Zhang J, Liu L (2017) Publicly verifiable watermarking for intellectual property protection in FPGA design. IEEE Trans Very Large Scale Integr (VLSI) Syst 25(4):1520–1527
19. Akhavan AA, Lim S-C, Hassan Z (2012) An image encryption scheme based on quantum logistic map. Commun Nonlinear Sci Numer Simul 17(12):4653–4661
20. Mohanty SP, Nayak S (2004) FPGA based implementation of an invisible-robust image watermarking encoder. In: Intelligent information technology, Springer, Berlin, pp. 344-353
21. Chroni M, Fylakis A, Nikolopoulos SD (2013) Watermarking images in the frequency domain by exploiting self-inverting permutations. J Inf Secur 4(2):80
22. Sharma G et al (2018) Publicly verifiable watermarking scheme for intellectual property protection using quantum Chaos and bit plane complexity slicing. Multimed Tools Appl 77(24):31737–31762
23. Chang CC, Hu YS, Lu TC (2006) A watermarking-based image ownership and tampering authentication scheme. Pattern Recognit Lett 27(5):439–446
24. Aroge TK, Isinkaye FO (2012) Watermarking techniques for protecting intellectual properties in a digital environment. J Comput Sci Technol 12(01):27–31
25. Adelsbach A, Sadeghi A-R (2001) Zero-knowledge watermark detection and proof of ownership. In: International workshop on information hiding, Springer, Berlin, pp 273–288
26. Wang Zhou, Bovik Alan C (2002) A universal image quality index. IEEE Signal Process Lett 9(3):81–84
27. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image process 13(4):600–612
28. Tehranipoor M, Wang C (eds) (2011) Introduction to hardware security and trust. Springer, New York
29. Beth T (1988) Efficient zero-knowledge identification scheme for smart cards. In: Workshop on the theory and application of cryptographic techniques, Springer, Berlin, pp 77–84
30. Huynh-Thu Q, Ghanbari M (2008) Scope of validity of PSNR in image/video quality assessment. Electron Lett 44(13):800–801

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.