Journal of Ambient Intelligence and Humanized Computing (2023) 14:2631–2643
https://doi.org/10.1007/s12652-022-04510-8

ORIGINAL RESEARCH

CADEN: cellular automata and DNA based secure framework for privacy preserving in IoT based healthcare

Nasir N. Hurrah[1] · **Ekram Khan**[1] · **Uzma Khan**[2]

Received: 21 May 2022 / Accepted: 13 December 2022 / Published online: 26 December 2022

Abstract
In the present E-healthcare industry, data breaches result in substantial economic losses due to cyber-attacks and hence create a trust deficit between the industry and users. The healthcare industry has rapidly adopted IoT frameworks but the trust deficit and privacy concerns limit its utilization among the masses. Along with privacy protection, content authentication is an important requirement in a number of critical applications and fragile watermarking provides an effective solution. However, existing fragile watermarking techniques lack the accuracy of tamper detection and hence are not reliable enough in terms of security and privacy of the data. This paper presents a novel low-complexity block-based fragile watermarking technique with high security against cyber-security attacks. This is achieved by embedding a fragile watermark in the host image using pixel domain blocking approach. The security of embedded watermark has been taken care of by using Cellular Automata and DNA based ENcryption (CADEN) framework to scramble the watermark bits using various secret keys. Experimental investigations show that besides being highly secure, the proposed technique is fragile to various signal processing and geometric attacks. The comparative analysis shows that the proposed scheme, despite having lower complexity, offers better efficiency in terms of imperceptibility, tamper detection and localization compared to other state-of-the-art techniques. Besides, the fragile watermark embedding makes the system capable to preserve the secret information in case of an attack with an average BER of 40%.

Keywords Cyber security · Internet of medical things · Data protection · E healthcare · DNA encryption · Spatial domain watermarking · Fragile watermark

1 Introduction

With the global impact of Covid 19, there has been a paradigm shift in every domain and the adoption of technology has increased than never before. This has been aided by the new platforms put forward with the advent of different technologies like artificial intelligence (AI), blockchain technology, industrial cyber-physical systems (ICPS), internet of things (IoTs), smart power grids, autonomous control systems and the combination of all i.e., Industry 4.0 (Tang et al. 2020; Vanchinathan et al. 2021). These technologies rely upon various state-of-the-art algorithms to carry out numerous tasks and control operations in the automated environment without human intervention (Hurrah et al. 2021; Kumarasamy et al. 2021). For the implementation of these technologies plethora of data is exchanged between various systems, sensors, and cloud to carry out the desired tasks. However, this data exchange has given rise to many cybersecurity issues due to unauthorized tampering, data breaches, ransomware attacks, and other issues due to noise in communication channels, malfunctioning of devices, and data errors; which effect the decision-making of these smart systems (Milano and Gomez-Exposito 2020; Zhang et al. 2017).

The adoption of IoT-based services in healthcare industry, i.e., IoT for E-healthcare also known as IoMT, promises to bring biggest technological delivery to carry out several automated tasks in the medical diagnosis (Shah et al. 2022). In an IoMT environment large number of cameras and sensors continuously capture images and share other electronic health records (EHR) like X-ray, CT Scan MRI images etc.,

✉ Nasir N. Hurrah
hnasirg01@gmail.com

[1] Department of Electronics Engineering, Aligarh Muslim University, Aligarh, UP, India

[2] Department of Higher Education, Srinagar, J&K, India

through a network for real-time monitoring and diagnosis (Sun et al. 2021). This also includes diagnostic reports and other electronic patient information (EPI). However, the adoption of IoMT is gradual due to multiple constraints, one being trust deficit due to privacy concerns and other being resource-constrained devices (Hurrah et al. 2019a). In an IoMT environment where private data is shared along with other medical reports, the data breach can compromise the identity of the patient. A microscopic alteration could expose the identity of a subject or produce erroneous information for diagnosis and hence altering the decision-making of a system in IoMT framework (Yan et al. 2022). As per reports, the data breaches increased by 17% in 2021 compared to 2020 and resulted in substantial economic losses in billions of dollars, and critically affect millions worldwide. In 2022 there has been more rise in healthcare breaches and as per Ponemon Institute and Verizon Data Breach Investigations Report, the health industry suffers most from data breaches than any other sector (CIS 2022). This necessitates the development of new techniques to reinforce the current cyber security frameworks in order to guarantee the authenticity, integrity, protection, and confidentiality of multimedia content. However, despite the introduction of numerous data privacy approaches in recent years, real-time secure data exchange has not yet been accomplished.

Of late various technologies like steganography, hashing, cryptography, watermarking, etc., have been proposed to counter the security and privacy issues (Tang et al. 2020). Digital watermarking serves as one of the effective tools for authentication and integrity of data (EPI) (Anand and Singh 2021). Digital watermarking is a data-hiding technique in which a watermark, or secret information, is concealed in a cover media so that only authorized users may access it. Similar to watermarking, significant research has been conducted on a number of cryptographic techniques, including homomorphic encryption, differential privacy, safe aggregation, federated learning, and some biologically inspired systems, to assure data privacy (Zhao et al. 2020; Meiser et al. 2022). Though cryptography is being used as an effective solution for issues pertaining to security, but the availability of powerful cryptographic tools result in unauthorized access and forgery of the data (Hurrah et al. 2021). However, if the two techniques, digital watermarking and cryptography, are used in combination, both data authentication and a high level of security can be provided to the multimedia data. The idea is to hide the sensitive information related to a person or any other subject in the related multimedia file in encrypted form. This will ensure that even in case of any cyber-attack, the sensitive information remains protected. Conventional digital watermarking techniques does not offer an ample level of data integrity against various attacks and the designs are usually computationally inefficient. In such a scenario, techniques need to be developed which offer high degree imperceptibility, high capacity, security to the embedded data, at a low computational cost (Sun et al. 2021; Hurrah et al. 2019a).

In this paper, a new computationally efficient approach is proposed for information security, data authentication and tamper localization. We make use of a DNA encryption in combination with Cellular Automata to scramble the information (EPI) before embedding which effectively counters an adversary and safeguards the illegal access of the sensitive information. The content authentication is effectively ensured with the spatial domain fragile watermarking approach. Different signal and image processing attacks like noise addition, filtering, compression, rotation, cropping, etc., are used for performance evaluation of the proposed scheme extensively. The experimental results obtained prove the efficacy of the technique and verifies its applicability in IoMT applications where security is of prime importance.

Rest of the paper is organized as follows. In Sect. 2 related work is discussed. Section 3 discusses in detail the proposed fragile watermarking framework. In Sect. 4 experimental results are demonstrated and detailed analysis of the proposed technique is carried out. The conclusion is presented in Sect. 5.

2 Related work

The research for security of confidential data has taken a long leap in recent past and as such, no technique has achieved a desirable performance due to evolving cyberattacks. For protection of multimedia data like medical images and other EHR in an IoMT framework, digital watermarking has turned out to be the most effective technique as it ensures tamper detection, authentication, data integrity, and protection of EHR. For example, for copyright protection and tamper detection, a transform domain-based watermarking approach has been presented in (Sanivarapu 2022). The authors have embedded 16-bits in the cover image for authentication of the watermark. There is no procedure for tamper localization in the technique. A similar technique has been proposed for authentication purposes (Kabir 2021). Although the technique effectively detects some of the tampering attacks, the tamper localization capability is weak. Also, the use of 8 × 8 blocks results in poor tampering rates. Another technique, wherein Integer Wavelet Transform (IWT) is used for embedding, has been proposed for authentication purposes (Barani et al. 2019). However, the use of two transform domain techniques viz IWT and SVD increases its computational cost. Also, from the results it is evident that the false positive (FP) and false (FN) rates are high, thus tamper detection is not accurate. An efficient CNN-based approach for copy-move image forgery detection has been proposed in (Koul et al. 2022). The approach although efficient, but has the limitation that it is applicable only for fixed number of images present in a dataset. In addition to this, the tamper detection is poor as FPR and FNR rates are high.

In recent years, various cryptographic techniques have been proposed for security of private data. However, in most of the real-time applications like IoMT, the data acquisition and transmission devices are lightweight and constrained in terms of resources (Shah et al. 2022; Anand and Singh 2021). It can be found that most of the recent cryptographic techniques use highly complex single or multi-dimensional chaotic systems. Also, the secret keys which provide actual security are limited in size and number which favours the cyber-attacks.

To establish a better computational efficiency, the digital watermarking techniques implemented in the spatial domain yield better performance. In the spatial domain, the authentication data is embedded by modifying the pixels of the image directly which reduces the computational cost as compared to the transform domain. In Kim and Yang (2021), a spatial domain technique uses two LSB bits for embedding of data, which reduces the quality of the stego image. However, there is both threat of data breach as keys are sent along the stego image data along with high possibility of extraction failure due to bit errors that occur in the transmission network. Also, there is no provision for tamper localization which is necessary to check the nature of attacks. To preserve the privacy of the confidential information, a combination of chaos and a steganography-based framework has been proposed in Rostam et al. (2022). The authors have used block centers to generate the secret keys needed during chaotic encryption of the information and randomly selected pixels from a random are used for embedding. Although the framework effectively hides the information in the cover image, the quality of the watermarked images is less and there is no procedure to detect an attack for authentication purposes. A spatial domain-based watermarking approach based on embedding through a hash-based approach is proposed in Bhalerao et al. (2021) In this approach, SHA-1 hash function is used to calculate the hash of 4 × 4 block pixels with LSB pixels reset and the hash key code generated is embedded in the LSBs. Although the technique effectively detects every tamper, the False Positive Rates (FPR) calculated are not accurate enough. The reason for this is the selection of 4 × 4 block and as such even if one pixel is tampered the technique returns the detection of tamper for the whole block comprising of 15 un-tampered pixels. In addition to this, there is no mechanism to hide a secret information, so not suitable in IoMT applications. A better technique for tamper detection with electronic patient information hiding capability for medical Images is proposed in Lin et al. (2022). This technique however does not offer tamper localization and the fragility of the EPI is weak as demonstrated in various results. Table 1, presents the summary of the literature work. Other techniques like (Xiang et al. 2015; Singh and Singh 2017; Haghighi et al. 2018) suffer with similar limitations. To counter all the issues as reported in previous techniques and achieve better tamper proof framework for IoMT applications, we propose a new spatial domain-based watermarking approach as described in Sect. 3.

3 Proposed approach

The proposed technique is designed for IoT-based healthcare applications where highly sensitive EHR and EPI data is shared through public networks. To ensure the authentication of data shared through public networks, fragile watermarking approach has been adopted. The proposed technique ensures confidential data has high-level of security and fragility, and additionally tamper localization of the cover media. The proposed spatial domain, blind fragile watermarking approach has three main stages: encryption, embedding, and extraction stages.

In the encryption stage, security keys are computed as required for the encryption of the confidential information (EPI), embedded as watermark logo ‘L’. To enhance the security to an unbreakable level we encrypt the logo using two encryption systems, which are computationally

Table 1 Work done in various related papers

Scheme	Sanivarapu (2022)	Kabir (2021)	Barani et al. (2019)	Koul et al. (2022)	Rostam et al. (2022)	Bhalerao et al. (2021)
Embedding	Robust	Fragile	NA	NA	NA	Fragile
Authentication	Yes	Yes	Weak	Strong	No	Yes
Localization	No	Poor	Poor	No	No	Poor
Complexity	High	High	High	Medium	Medium	Low
Detection	Blind	Blind	Blind	Medium	No	Blind
Security	Yes	Yes	Yes	No	Yes	Yes

efficient and even if one gets compromised other ensures the security. In the embedding process, the distortion due to watermark is kept to the LSBs of the pixels which ensures no significant distortion in the cover image. For integrity authentication, the values of the pixels from the block are used to compute various parameters that decide the embedding along with the watermark bit. Finally, the calculated bit stream is added to the LSBs of selected block pixels to get the final watermarked image. On the receiver side, we can extract the embedded watermark bits and authenticate whether the image is attacked, recover the watermark in case of no attacks, or directly discard the information in case of an attack. The complete approach adopted in proposed technique is broadly categorized in three steps as:

(1) Encryption of the secret information in the pre-processing stage, discussed in Sect. 3.1;
(2) Embedding of watermark in the cover image, discussed in Sect. 3.2; and
(3) Extraction of the watermark to recover the embedded information and localize the tamper in case of an attack, which is covered in Sect. 3.2.2.

3.1 Watermark scrambling

The watermark is first forwarded to the encryption stage, and the corresponding encryption algorithms are applied to determine the level of encryption. The level of watermark encryption is a function of various secret keys and the formulated algorithm. To ensure better security, in the present work, a hybrid combination of encryptions involving DNA and Cellular Automata is applied. The scrambling of the watermark is done by a set of pre-defined rules, which acts as the unique key for encryption.

3.1.1 Elementary cellular automata

Recently, there has been large scale adoption of nature inspired algorithms to increase performance of various system processes in different domains of technology (Ping et al. 2022; Vanchinathan and Selvaganesan 2021). Proposed work adopts Cellular Automata (CA) based algorithm, a computational model typically represented by a grid of cells, for encryption of information. The state (value) of a cell in the grid is a function of the previous neighborhood state and some rule. The behavior is pseudo-random and hence best suited for encryption. The Elementary CAs are formed by evolving a row of cells according to a rule into multiple rows with each row stacked below the predecessor as shown in Fig. 1. In Fig. 1a we have shown three representations with the evolutions of 128 (i.e. 128 rows and the initial state is all zeros except for a 1 at the central element) of the CA. The CA is extremely sensitive to initial conditions and changing a single bit can change the entire representation as described in Fig. 1. For this reason, Elementary Cellular Automata (ECA) can be used effectively to encrypt the watermark information. The ECA-based algorithm is used to iteratively encrypt the watermark information according to the selected balanced rules. In ECA three cells form a neighborhood and hence there are eight possible patterns. Now for each pattern, the rule decides whether the cell will be 0 or 1 in the next generation. Hence, there are 2^8 (256) rules that can define an ECA-based representation. The CA avoids the problem of dynamic degradation when implemented on digital devices compared to chaotic maps having finite computing precision (Ping et al. 2022) Because of their inherently simple hardware implementation, the CA-based encryption algorithms are used to generate random sequences. Also, since encryption involves only XOR operations the computational efficiency is very high. The process of encryption depends on the rule and each rule yields a specific pattern.

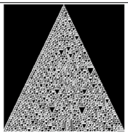
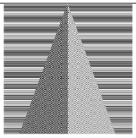
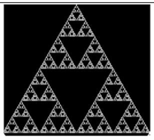
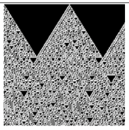
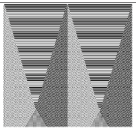
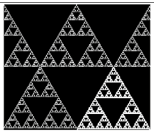
Rules	Rule 30	Rule 57	Rule 90
Initial sequence with all zeros and only middle bit 1			
One bit of the initial sequence changed to 1			

Fig. 1 Various rule-based patterns of ECA

3.1.2 DNA encryption

Originated from biology, the DNA (Deoxyribonucleic acid) carries the genetic data of the biological characteristics (Meiser et al. 2022; Sha et al. 2021). DNA is composed of two polynucleotide strands where each nucleotide contains one of four nitrogenous bases: Adenine ‘A’, Cytosine ‘C’, Guanine ‘G’, and Thymine ‘T’. DNA encryption involves the representation of a binary sequence in terms of these nucleotides. The DNA version of the information is then permuted by other operations to form a scrambled sequence which is difficult to be decrypted by unauthorized users. Using these four bases to encode bit pairs 00, 01, 10, and 11, there are 24 kinds of coding schemes. However, in actual DNA-based structure, A and T are complementary, G and C are complementary. Similar to the binary system where 0 and 1 are complementary, the binary pairs 00 and 11 are complimentary, and likewise is the case of 01 and 10. Adapting the Watson–Crick complement rule as done in the previous works, there are only 8 different possible coding schemes, as shown in Table 2. It is pertinent to mention here that we will not follow only the Watson & crick rules as done in all other previously proposed techniques based on DNA encryption. This is due to the reason that using only a key set of 8 rules has less advantage in the data encryption process as compared to ambiguity created by adopting all the rules. So, keeping all the rules concerned with combinations of the DNA bases at the disposal of the designer creates additional ambiguity in the data.

3.1.3 Encryption procedure

In this work, we take a binary watermark of size n × n bits for embedding in the cover image. Zigzag scanning is applied to construct a 1D array of bits from the watermark logo. The encryption of the watermark is done by scrambling the group of ‘n’ (say) bits with the sequence obtained by applying Cellular Automation and DNA-based cryptographic procedure. With 256 rules of ECA and 24 rules of DNA, the total set of rules available for encryption is 24^{256}. The idea of designing a cryptosystem made of DNA molecules is proposed to formulate a technique that is in principle unbreakable (Meiser et al. 2022). In addition to this, the randomly selected column from the ECA matrix acts as a secret key to encrypt the watermark. The idea is to encode secret information into the four nucleotides of DNA, subsequently mixing the message-DNA with human genome DNA before embedding. With the knowledge of both the procedure and the encryption keys, the authorized recipient could decipher the DNA message. Considering a binary watermark of size 128 × 128 for the demonstration of the proposed encryption approach. At first, key (K_{CA}) with length of 128 bits is obtained from column 127 (say) using Rule ‘R_2’ of ECA and these bits XOR the first 128 bits of the watermark obtained by a zigzag scan of the matrix. The rest of the 128-bit combinations of the watermark are obtained by performing the DNA operation of the subsequent 128 bits. Each of these 128 watermark bits is used to XOR the key (K_{CA}). Here the rules of DNA for next watermark 128-bits combinations are adaptive depending on the decimal equivalent (W_E) of the 128-bit watermark result of previous XOR operation and selected by using the following operation:

$$\text{Rule}(R) = 1 + \text{mod}\left(W_E, 8\right) \tag{1}$$

Here we divide the 128 bits of the information into 8-bit groups to apply our DNA-based rules. Like the interaction of chromosomes in a living body, we adopt a similar approach to obtain the random crossover of the nucleotides in the two DNA strands. This random crossover enables us to obtain a system with a high level of security.

Following steps are followed for the complete encryption of the watermark information.

1. Perform a zigzag scan to construct the array from the watermark of size n × n.
2. Encrypt the first 128 bits of the watermark array by Rule (R_1) of DNA and perform an XOR operation with a random sequence (K_{CA}) obtained from Cellular Automata with another secret rule (R_2), say rule 30. The resulting sequence is also stored in a buffer and forwarded. Both the rules act as secret keys of encryption process.

Algorithm 1: Proposed Encryption Algorithm

```
Input: Private data (I), Private Keys, Rules ($R_1$, $R_2$), n
    Initialize: j = 1, x = 1, y = n
    Z = zigzag (I)
    $C_j$ ← $E_{DNA}$(Z(x:y), R1)
    $S_N$ ← $S_{ECA}$($R_2$)
    $X_1$ = $C_j$ ⊕ $S_N$
    FOR X, y
        j = j+1
        $C_j$ ← Z(x: y)
        $C_j'$ ← $E_{DNA}$ ($C_j$, R)
        $X_j$ = $C_j'$ ⊕ $S_N$
        Increment: x = x + n, y = y + n
    END FOR
Output: Encrypted data: $I_s$ ← $X_j$
```

3. The next 128 bits of the watermark are first applied with DNA encryption. This encryption is done by first arranging the bits in blocks of length 8-bits. Each block

Table 2 Eight complementary rules of DNA bases

DNA bases	Binary representation for eight rules (D_C)							
	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8
A	11	11	10	10	01	01	00	00
T	00	00	01	01	10	10	11	11
C	10	01	00	11	00	11	10	01
G	01	10	11	00	11	00	01	10

Table 3 XOR operation on DNA bases

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

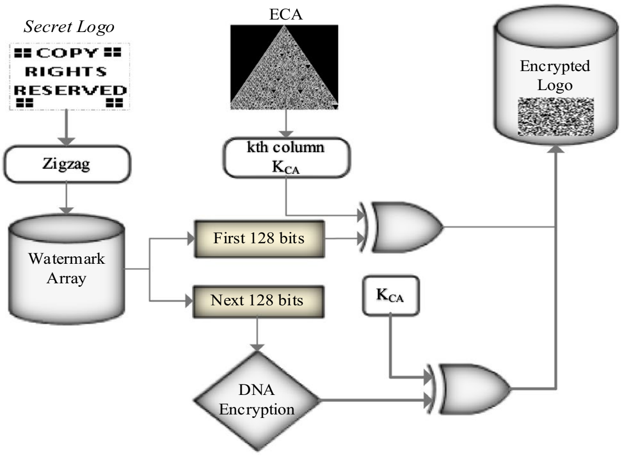


Fig. 2 Block diagram for encryption of secret information

is converted to a DNA sequence by employing Table 1 where rule selection for each block is done using Eq. (1). At the same time, the 128-bit sequence (K_{CA}) is XORed with this sequence to get the final 128-bit sequence. The procedure for XOR operation is shown in Table 3.

4. The result of step 3 is again stored in a buffer and encryption of the next 128 bits is done by similar procedure as described in Fig. 2.

5. The groups of 128 bits encrypted sequences are concatenated together to form a final encrypted sequence.

3.2 Watermark embedding and extraction procedure

The proposed watermarking procedure is demonstrated in Fig. 3. It is based on the pixel modification in the spatial domain. In the proposed approach of embedding, each block of the cover image is read in order and the pixel selection is done in an ordered manner using a pre-defined concept set for sub-block creation during the design process. The proposed approach involves the calculation of various parameters from the selected image sub-block pixels as described in Sect. 3.2.1. These parameters like 'Sum', 'Mod' etc. decide the fragility of the watermark and in case of an attack the changes are reflected in these parameters which result in extraction of incorrect information bit. The computed parameters decide the modification of LSB bits. The computed bit sequence from the selected pixels is used to replace the original LSB bits. Since ECA and DNA algorithms are used in the preliminary stages for scrambling, the same procedure is applied to extract the secret information.

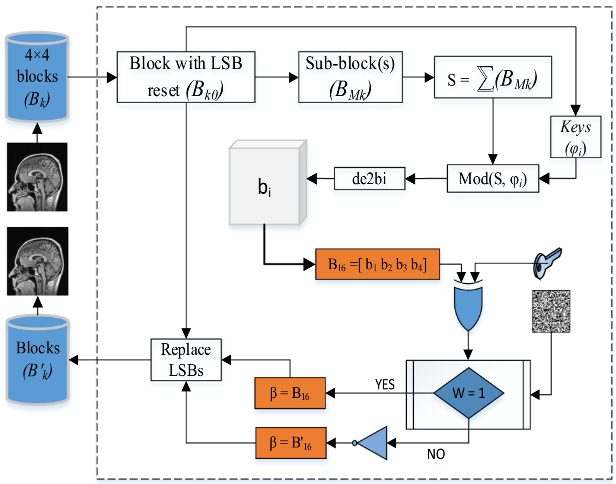


Fig. 3 Block diagram for embedding watermark

3.2.1 Embedding algorithm

The embedding algorithm involves spatial domain-based watermark hiding procedure. Here, we hide secret information and tamper localization bits together as watermark in the cover image. Figure 3 presents the block diagram of the proposed watermarking methodology and is illustrated in Algorithm 2. Figure 4 shows embedding procedure for a block with an example.

Step 1: Apply the encryption algorithm proposed in Sect. 3.1.3 to the secret information.

Algorithm 2: Watermark Embedding

```
Input: $B_K$, Key
Output: $B_K'$
For each $B_K$
        pre-process: $b_1$, $b_2$, $b_3$, $b_4$
        concatenate $B_{16} \leftarrow [b_1\ b_2\ b_3\ b_4]$
            $\beta \leftarrow B_{16} \oplus Key$
        if w == 0
                $\beta = \overline{\beta}$
        end
                LSB ($B_K$) $\leftarrow \beta$
End For
```

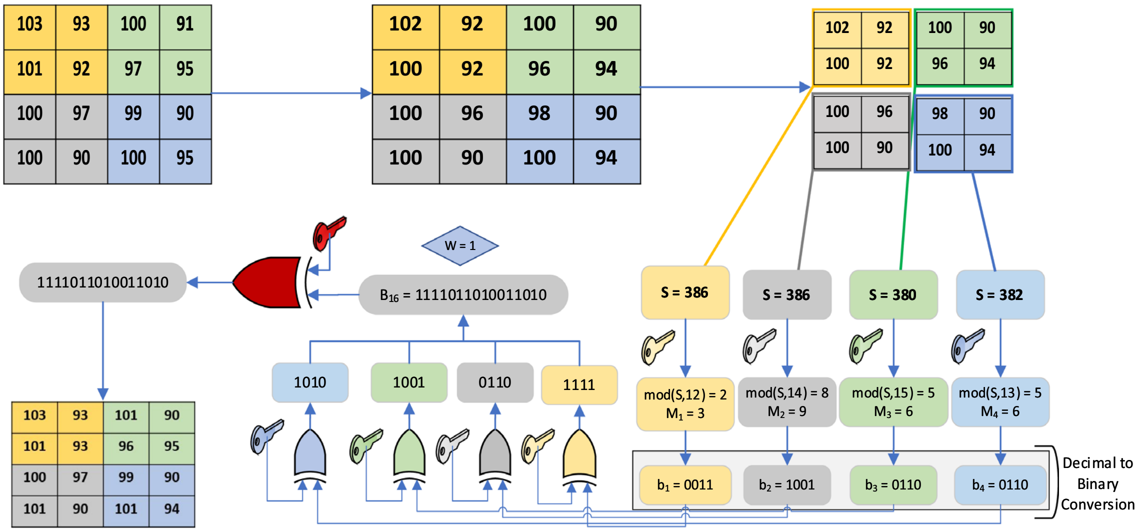


Fig. 4 The flow of watermark embedding in a block

Step 2: Divide the cover image into 4 × 4 blocks and represent blocks by 'B_K' as shown in Fig. 3.

Step 3: Reset the LSBs of each pixel in block Bk to zero, and resulting block is represented as B_{k0}.

Step 4: Divide the block into four sub-blocks of the size of (2×2=) 4 pixels, each represented by 'B_{MK}'. Calculate the sum of all the pixels of each sub-block and represent as S as given in Eq. (2).

$$S = \sum B_{MK} \tag{2}$$

Step 5: Calculate the modulus of the sum and perform decimal to binary conversion using a different key for each sub-block. These keys (φ_i) are numbers with value $11 < \varphi_i < 16$ and are calculated from B_{K0}.

$$\begin{aligned} M_K &= 1 + \text{mod}(S, \varphi_i) \\ b_K &= M_K \rightarrow binary \end{aligned} \tag{3}$$

Obtain the final 4-bits of each sub-block and store them in the arrays b_1, b_2, b_3 & b_4 respectively. Concatenate all the resulting bits into a 16-bit sequence and perform an XOR operation with another secret key to get the final 16-bit sequence to be embedded in the LSB pixels to get the watermarked sub-block.

Step 6: For each 4 × 4 block, one bit (I_b) of the secret information (I) is embedded in the LSBs using the following equation.

$$LSB(B_k) = \begin{cases} \beta \ if \ I_b \, is \, 1 \\ \overline{\beta} \ if \ I_b \, is \, 0 \end{cases} \tag{4}$$

Step 7: The resulting bits in step 6 replace the LSB bits of the corresponding pixels in the 4 × 4 block.

Step 8: This completes the embedding process in a block and results in a modified block carrying watermark information**.**

3.2.2 Blind watermark extraction

In the proposed system, for the extraction of watermark, preprocessing for image preparation follows same set of steps as done for embedding. The watermarked image is subjected to same pre-processing procedure as described in Sect. 3.2 to extract blocks. The decryption algorithm and corresponding keys are generated for the decryption of the extracted data. Figure 5 shows the procedure for extraction of information and the tamper detection procedure.

In the figure each 4×4 block is pre-processed same way as done during embedding stage. For each block XOR operation is performed between the 16-bit factor B_{16} and corresponding extracted LSB bits. The number of ones present in result, B_x, are stored in parameter 'η'. Clearly, if all the bits in B_{16} and corresponding extracted LSB bits are same or different, the parameter 'η' is equal to zero or 16. In this case the block is considered untampered. Now, depending on the value of 'η' being 0 or 16 we decide whether the secret data bit is 0 or 1. In case, $\eta = 0$, the secret data bit is 1 and if $\eta = 1$ then secret data bit is 0. Now, in case there is any attack, the value of 'η' being any number other than 0 or 16 detects that block has been tampered.

So, in case 4×4 block is detected as tampered, a next level tamper detection is done on its corresponding 2×2 sub-blocks. This is done by comparing LSB bits 'L_i' of that block with corresponding 'b_i' values. The number of zeros (N_z) computed for each 2×2 block, decide whether the sub-block is tampered or not.

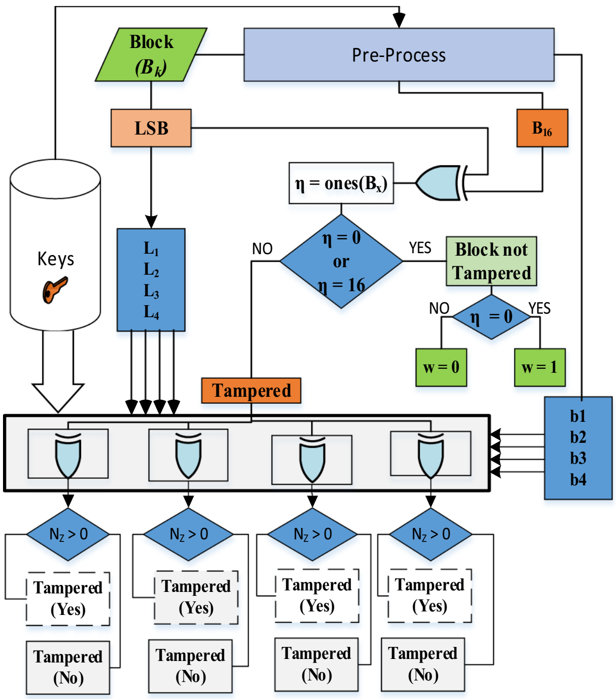


Fig. 5 Tamper detection and watermark extraction framework

4 Experimental results and discussion

The evaluation of the proposed fragile technique has been performed on various types of standard grayscale and medical images. The test images have been retrieved from the databases (USC-SIPI 1977; OPENi 2022). MATLAB R2019a is used to perform both subjective and objective analyses. For all the experiments, a binary image of size 128 × 128 (16,384 bits) is used as a secret information. In this article, we have only shown the images which are used to compare the results with some of the state-of-the-art techniques. These test images are shown in Fig. 6. From the results, it has been established that the proposed fragile watermarking technique demonstrates better performance compared to previously developed techniques for the purpose and hence can be effectually used for privacy preserving in various applications. The subjective analysis is performed using PSNR (peak signal to noise) as imperceptivity parameter. Similarly, the parameters BER (Bit error rate) and Normalized Cross-correlation (NCC) are used for fragility analysis (Hurrah et al. 2019b).

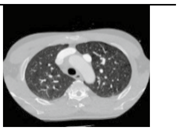
Watermarked Standard Images			
PSNR (dB)	51.24	51.13	51.22
Watermarked Medical Images			
PSNR (dB)	51.09	51.17	51.23

Fig. 6 Some of the test images used in the proposed scheme

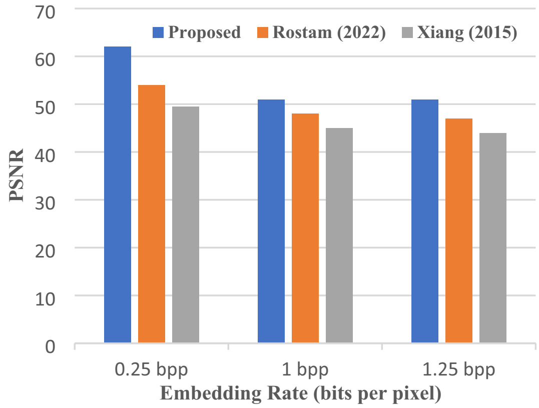


Fig. 7 Quality analysis at different embedding rates

Figure 6 shows the results in terms of PSNR for various images. It is evident from the figure that the proposed technique achieves very high imperceptibility results as PSNR more than 51 dB when embedding 16 bits of recovery data per block along with total of 16 kb secret data in the cover image of size 512 × 512.

The proposed technique achieves an average PSNR above 51 dB for embedding 1bpp. A comparison has been performed with (Rostam et al. 2022; Xiang et al. 2015) in Fig. 7 in terms of PSNR. In this perspective, comparison is done with data of size 0.25 bits per pixel (bpp), 1.25 and 1 bpp using the cover image of size 512 × 512 pixels. It can be seen from the Fig. 7 that proposed technique has better imperceptivity as compared to other techniques under comparison. Unlike, our approach where only LSB bit is modified, the techniques under comparison modify other bits in addition to LSB bit of a pixel which deteriorates visual quality. For embedding less than 2 bpp these techniques select some of the pixels in a block and modify the two LSBs of selected pixels by secret data bits. However, this decreases the visual quality of the cover image in the process.

4.1 Fragility watermarking results

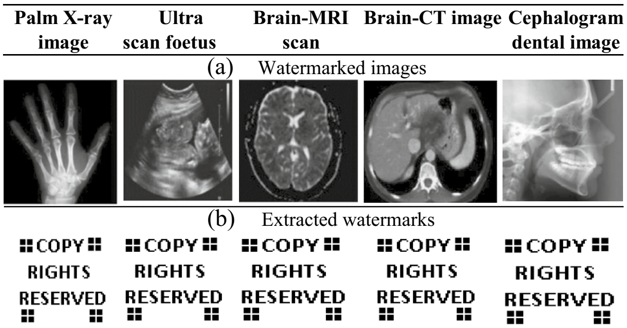
In this section, the fragility analysis to check the level of sensitivity towards various attacks is evaluated. The purpose of embedding a watermark with the fragile technique is to ensure authentication in presence of various forgery attacks. In the analysis we have considered various tampering attacks for image manipulations due to filtering, cropping, scaling, adding noise, and so on. Both subjective and objective results are presented. The parameters used for the evaluation are NCC and BER, evaluated with respect to the original and the extracted watermark.

It is pertinent to mention here that our technique has capability of detecting tempering of pixels in 2×2 blocks as compared to 4×4 block-based techniques under comparison. This results in a better tamper detection rate otherwise interpreted wrongly by 4×4 block fragile techniques. This ensures the pixels at the boundaries of the tamper region are not falsely detected tampered as found in 4×4 block-based authentication techniques where a single pixel modification in a 4×4 block returns other 15 untampered pixels as tampered during detection. In comparison, our technique detects the tampering for a 2×2 block, so in case a single pixel is corrupted, only three untampered pixels are wrongly detected as tampered.

The proposed scheme has been evaluated for various performance parameters commonly used for analysing fragility in attack scenario. Figure 8 shows the results in terms of NCC and BER for various images under no tampering attack. It is evident from the figure that the proposed technique is able to extract watermark information without any error as the value of BER is zero. The higher BER and lower NCC demonstrates that more of the information bits get destroyed and the correlation highly reduces between the extracted and original information.

Watermark fragility is one of the most important parameters that can estimate privacy and authentication during the data exchange. Fragility of a watermarking scheme is analysed by testing the algorithm under several possible attacks and recording the results under controlled environment. Figure 9 presents the results obtained by the proposed technique in presence of copy-move and crop attack, and copy-paste and constant-average attack.

It is clear from the results in Fig. 9 that the proposed algorithm accurately detects the tamper and there is no meaningful information extraction, which establishes the high fragility performance of proposed scheme and thus can be used for authentication applications.



BER	0	0	0	0
NCC	1	1	1	1

Fig. 8 Extracted watermark logos for various watermarked medical images and results in terms of NCC and BER values

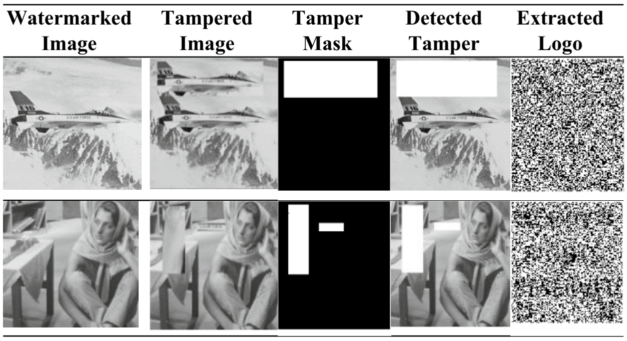


Fig. 9 Watermarked images, tamper localization results and extracted watermarks

Figure 10 presents the results for various attacks applied on the watermarked image. It can be seen from the results that in case of every attack the secret information embedded via a binary logo gets completely destroyed, hence confirms that the proposed technique is highly fragile. In Fig. 11, a comparison has been presented with Lin et al. (2022) for six medical images, to check the performance in presence of various attacks in terms of NCC and BER. It can be seen that proposed technique offers better fragility as average BER of the extracted watermark is higher and average NCC is lower than Lin et al. (2022), for all the attacks except for JPEG with QF equal to 90 where results are weaker.

4.2 Tamper localization results

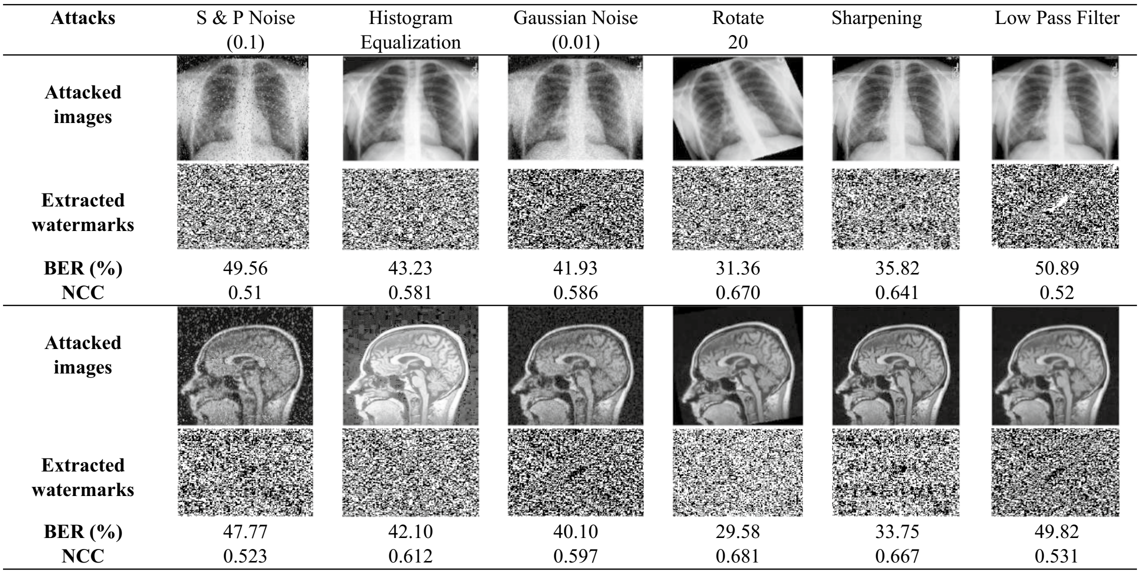
In this sub-section, the watermarked images have been tested for tamper localization accuracy and the results are presented for various attacks. We have incorporated multiple other parameters to calculate the objective quality of the proposed scheme. The parameters included for the calculation of accuracy are tamper detection rate (TDR), false-positive rate (FPR), and false-negative rate (FNR). The proposed scheme returns an accurate TDR of 100% for attacks like cropping, copy-move, copy-paste, etc.

$$TDR = \frac{Tampered\ Pixels\ Detected\ (T_D)}{Total\ number\ of\ tampered\ pixels\ (A_T)} \times 100\%$$

Although the parameter TDR checks the rate at which tampered pixels are detected, the actual rate at which pixels.

are tampered is accurately computed using parameters, FPR and FNR described below.

$$FNR = \frac{Pixels\ falsely\ Detected\ as\ Untampered\ (F_{DU})}{Actual\ number\ of\ Untampered\ Pixels\ (A_{UT})} \times 100\%$$



Attacks	S & P Noise (0.1)	Histogram Equalization	Gaussian Noise (0.01)	Rotate 20	Sharpening	Low Pass Filter
Attacked images						
Extracted watermarks						
BER (%)	49.56	43.23	41.93	31.36	35.82	50.89
NCC	0.51	0.581	0.586	0.670	0.641	0.52
Attacked images						
Extracted watermarks						
BER (%)	47.77	42.10	40.10	29.58	33.75	49.82
NCC	0.523	0.612	0.597	0.681	0.667	0.531

Fig. 10 Extraction of secret logo under different attacks

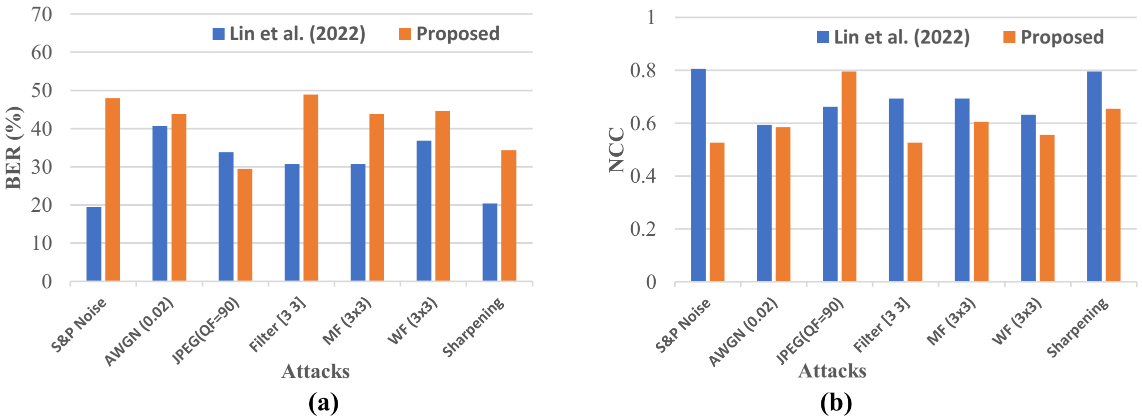


Fig. 11 Comparison with Lin et al. (2022) under different attacks, **a** in terms of BER (%), **b** in terms of NCC

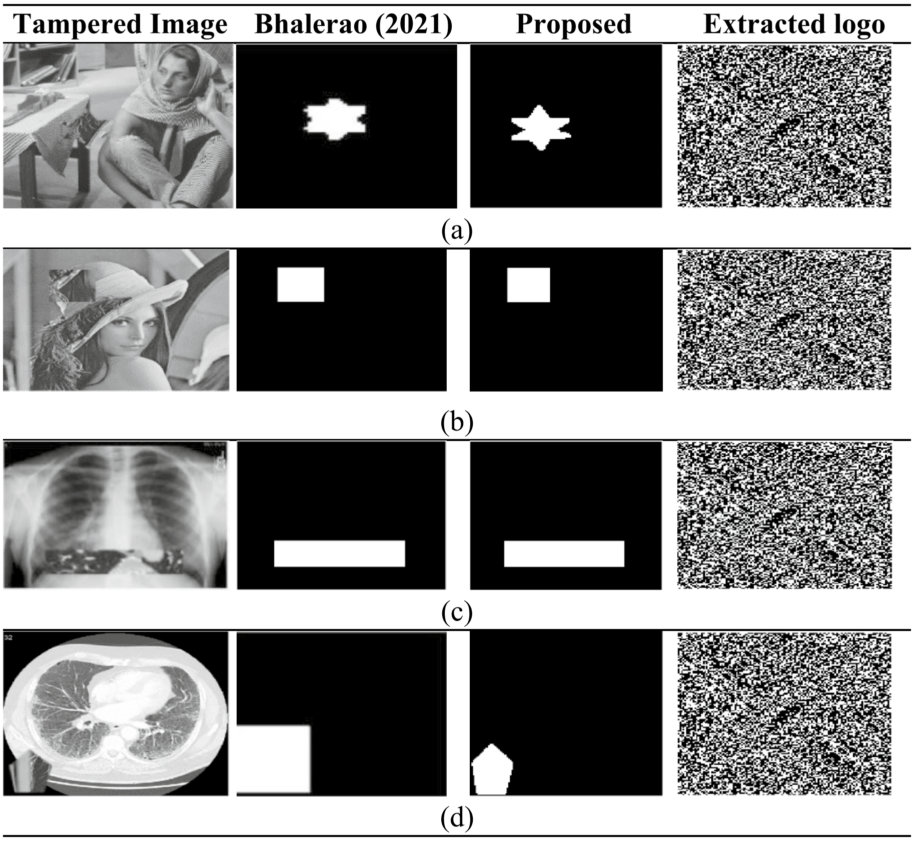
$$FPR = \frac{Pixels\, falsely\, detected\, as\, Tampered\, (F_{DT})}{Actual\, Number\, of\, Tampered\, Pixels\, (A_T)} \times 100\%$$

We have compared our technique with Bhalerao et al. (2021), for various attacks and the results are presented in Fig. 12. It is evident from the results in Fig. 12, that for the attacks presented in Fig. 12a, d, the proposed technique out performs the technique under comparison as tamper localization is better. Also, the extracted watermark in every case is completely destroyed which confirms the fragility of the watermark.

In Table 4 we have considered the different attacks and level of percentages for 20 images from USC-SIPI database. It can be seen from the Table 4 that the proposed technique results in high rate of tamper detection. The FNR is almost zero for every attack except in case of copy move attack where there is slight weakness in tamper detection for when tampering percentage is more than 25%. However, this is less than 1% and since authentication watermark bits get destroyed in every case there is no issue with respect to detection of tamper.

The results in the Table 4 give an estimate of performance of the proposed scheme in terms of falsely detected pixels for attacks like copy-paste, copy-move and random tampering. It is pertinent to mention here that the proposed technique involves the size of the block as 2×2 at the second level of detection. Hence compared to technique under comparison, the proposed technique with the block size of 2×2 the FPR is less, as shown in Fig. 13.

Since both schemes, proposed and Bhalerao et al. (2021), are block-based methods, a single pixel tampering returns detection as whole block as tampered. Clearly, for less



(a)

(b)

(c)

(d)

Fig. 12 Comparison for: **a** General tampering, **b** copy-paste attack, **c** copy-move attack, **d** constant average attack

Table 4 TDR, FPR and FNR results of proposed scheme for different tampering attacks

Tampering (%)	Random tampering			Copy move			Copy paste		
	TDR	FPR	FNR	TDR	FPR	FNR	TDR	FPR	FNR
1	100	12.15	0	100	13.33	0	100	12.36	0
5	100	7.5	0	100	9.54	0	100	7.43	0
10	100	5.59	0	100	6.93	0	100	5.81	0
15	100	1.45	0	100	5.46	0	100	2.43	0
20	100	0.66	0	100	3.27	0	100	0.71	0
25	100	0.47	0	100	2.25	0.03	100	0.52	0
30	100	0.43	0	100	0.76	0.04	100	0.50	0
35	100	0.41	0	100	0.63	0.04	100	0.45	0
40	100	0.37	0	100	0.57	0.04	100	0.41	0
45	100	0.32	0	100	0.54	0.05	100	0.38	0
50	100	0.31	0	100	0.48	0.05	100	0.33	0

tampering percentages, the number of pixels falsely detected as tampered are more. The proposed model checks the tamper only in case of authentication at first level detects tamper, this approach saves a lot of computational time.

From Fig. 13, it is clear that the proposed method demonstrates better results in terms of FPR in comparison to the other method for attacks like random tampering (RT), copy-move (C&M) and copy-paste (C&P). For comparison with Bhalerao et al. (2021) we have considered the same formula as used by authors.

4.3 Timing analysis

The computational cost of a data hiding algorithm is computed in terms of embedding and extraction times. The computational complexity is an important parameter to evaluate efficiency and applicability of an algorithm in real-time applications. In order to establish the applicability of proposed technique for real time applications we have compared the proposed technique with some of the state-of-the-art techniques in literature. The results in

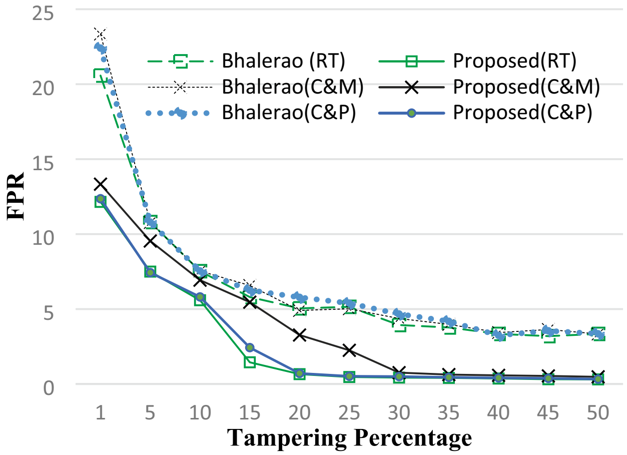


Fig. 13 Comparison of FPR with Bhalerao et al. (2021) for different tampering rates

Table 5 Comparison: embedding and extraction time

Approach	Avg. embedding time (s)	Avg. extraction time (s)
Singh (2017)	6.43	–
Haghighi (2018)	9.44	14.32
Barni (2019)	2.33	2.57
Proposed		
USC-SIPI	**1.53**	**1.71**
UCID database	**1.574**	**1.723**

terms of embedding and extraction times are displayed in Table 5.

It is evident from Table 5 that the proposed technique is faster due to its lower execution times. Our technique is implemented on MATLAB 2019a platform running on 2.4 GHz processor with 8 GB RAM. The lesser embedding and extraction times achieved by the proposed system, as presented in Table 5 are respective average times, computed for 100 images from USCSIPI database and 1338 images from the UCID database (Schaefer and Stich 2003).

4.4 Key analysis

The security of an information encryption system is analysed by testing the strength of the keys in adverse conditions. And as such secure and reliable system must possess keys of high sensitivity to resist various types of attacks with authority. The proposed encryption framework is designed by employing various secret keys in the form of initial values and rules. The ECA is employed with an initial sequence, a particular rule and sequence procedure.

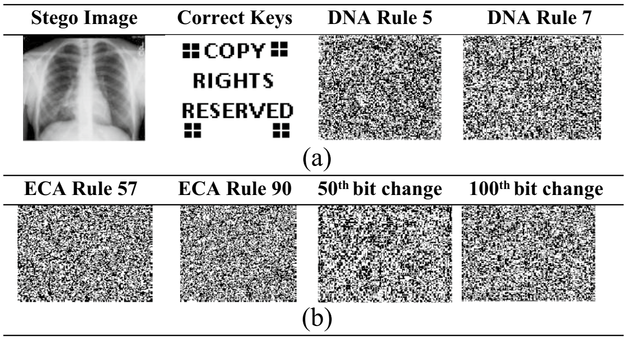


Fig. 14 Key sensitivity test results

In the proposed work, the initial values of the ECA is a 128-bit sequence and acts as a key of length 2^7. The randomly selected column of ECA matrix also acts as a key of length 2^7. The DNA encryption is also employed with a particular rule selected from 24 rules. In order to test the sensitivity of these keys, let's change bit at 50th and 100th position of the sequence, the results of watermark extraction are shown in Fig. 14. The result of rule change can also be seen from Figure. As can be seen, that a single bit-change in a key or a rule (Original DNA rule is Rule 8 and ECA Rule 30) variation will result in zero information extraction.

5 Conclusion

In this paper, a spatial domain-based blind fragile watermarking scheme for authentication of multimedia data has been proposed. Due to its fragility characteristics, it achieves high tamper detection and localization accuracy. The tamper detection accuracy achieved by the proposed technique is 100%. The localization accuracy analyzed in terms of TDR is near 100%. The experimental results establish that the proposed technique achieves high fragility against various commonly occurring attacks like cropping, histogram equalization, scaling, filtering, noise addition, and compression. The encryption of the data before embedding ensures high-level security and protection in case the embedding algorithm is compromised. The encryption algorithm presented in the proposed scheme is computationally efficient as compared to the chaotic systems used in most of the techniques. The better efficiency of the proposed technique compared to state-of-the-art establishes it to be the best candidate for authentication, privacy, and integrity of the data in applications like IoT-based E-Healthcare systems.

Acknowledgements This publication is an outcome of the work undertaken under Dr. D. S. Kothari Postdoc (DSKPDF) Scheme, University Grants Commission (UGC), Govt. of India.

Data availability Data will be made available by the corresponding author privately for academic and research purposes upon request.

References

Anand A, Singh AK (2021) Health record security through multiple watermarking on fused medical images. IEEE Trans Comp Soc Syst 9(4):1594–1603

Barani MJ, Valandar MY, Ayubi P (2019) A new digital image tamper detection algorithm based on integer wavelet transform and secured by encrypted authentication sequence with 3D quantum map. Optik 187:205–222

Bhalerao S, Ansari IA, Kumar A (2021) A secure image watermarking for tamper detection and localization. J Ambient Intell Humaniz Comput 12(1):1057–1068

CIS Report (2022) Data breaches: in the healthcare sector. Available at https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector

Haghighi BB, Taherinia AH, Harati A (2018) TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique. J Vis Commun Image Represent 50:49–64

Hurrah NN, Parah SA, Sheikh JA, Al-Turjman F, Muhammad K (2019a) Secure data transmission framework for confidentiality in IoTs. Ad Hoc Netw 95:101989

Hurrah NN, Parah SA, Sheikh JA (2019b) A secure medical image watermarking technique for E-healthcare applications. In: Singh AK, Mohan A (eds) Handbook of multimedia information security: techniques and apps. Springer, Cham

Hurrah NN, Loan NA, Parah SA, Sheikh JA, Muhammad K, de Macedo ARL, de Albuquerque VHC (2021) INDFORG: industrial forgery detection using automatic rotation angle detection and correction. IEEE Trans Ind Inf 17(5):3630–3639

Kabir M (2021) An efficient low bit rate image watermarking and tamper detection for image authentication. SN Appl Sci 3(4):1–17

Kim C, Yang CN (2021) Self-embedding fragile watermarking scheme to detect image tampering using AMBTC and OPAP approaches. Appl Sci 11(3):1146

Koul S, Kumar M, Khurana SS, Mushtaq F, Kumar K (2022) An efficient approach for copy-move image forgery detection using convolution neural network. Multimedia Tools Appl 81:11259–11277

Kumarasamy V, Ramasamy VK, Chinnaraj G (2021) Systematic design of multi-objective enhanced genetic algorithm optimized fractional order PID controller for sensorless brushless DC motor drive. Circuit World. https://doi.org/10.1108/CW-07-2020-0137

Lin CC, Chang CC, Kao WJ, Chang JF (2022) Efficient electronic patient information hiding scheme with tamper detection function for medical images. IEEE Access 10:18470–18485

Meiser LC, Nguyen BH, Chen YJ, Nivala J, Strauss K, Ceze L, Grass RN (2022) Synthetic DNA applications in information technology. Nat Commun 13(1):1–13

Milano F, Gomez-Exposito A (2020) Detection of cyber-attacks of power systems through Benford's law. IEEE Trans Smart Grid 12(3):2741–2744

OPENi medical image database from National Laboratory of Medicine (2022). Available at https://openi.nlm.nih.gov/

Ping P, Zhang X, Yang X, Hashems YAA (2022) A novel medical image encryption based on cellular automata with ROI position embedded. Multimedia Tools Appl 81:7323–7343

Rostam HE, Motameni H, Enayatifar R (2022) Privacy-preserving in the Internet of Things based on steganography and chaotic functions. Optik 258:168864

Sanivarapu PV (2022) Adaptive tamper detection watermarking scheme for medical images in transform domain. Multimedia Tools Appl 81:11605–11619

Schaefer G, Stich M (2003) UCID: an uncompressed color image database. In: Storage and retrieval methods and applications for multimedia 2004, vol 5307. SPIE, pp 472–480

Sha Y, Cao Y, Yan H, Gao X, Mou J (2021) An image encryption scheme based on IAVL permutation scheme and DNA operations. IEEE Access 9:96321–96336

Shah SHA, Koundal D, Sai V, Rani S (2022) 5G edge computing enabled internet of medical things. IEEE Trans Ind Inf 18(2):8860–8863

Singh D, Singh SK (2017) DCT based efficient fragile watermarking scheme for image authentication and restoration. Multimedia Tools Appl 76(1):953–977

Sun Y, Liu J, Yu K, Alazab M, Lin K (2021) PMRSS: privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare. IEEE Trans Ind Inf 18(3):1981–1990

Tang W, Li B, Barni M, Li J, Huang J (2020) An automatic cost learning framework for image steganography using deep reinforcement learning. IEEE Trans Inf Forensics Secur 16:952–967

USC-SIPI Image Database from University of South California (1977). Available at https://sipi.usc.edu/database/

Vanchinathan K, Selvaganesan N (2021) Adaptive fractional order PID controller tuning for brushless DC motor using artificial bee colony algorithm. Results Control Optim 4:100032

Vanchinathan K, Valluvan KR, Gnanavel C, Gokul C (2021) Design methodology and experimental verification of intelligent speed controllers for sensorless permanent magnet brushless DC motor: intelligent speed controllers for electric motor. Int Trans Electr Energy Syst 31(9):e12991

Xiang T, Hu J, Sun J (2015) Outsourcing chaotic selective image encryption to the cloud with steganography. Digital Signal Process 43:28–37

Yan F, Huang H, Yu X (2022) A multi-watermarking scheme for verifying medical image integrity and authenticity in the internet of medical things. IEEE Trans Ind Inf 18(12):8885–8894

Zhang K, Ni J, Yang K, Liang X, Ren J, Shen XS (2017) Security and privacy in smart city applications: challenges and solutions. IEEE Commun Mag 55(1):122–129

Zhao Y, Zhao J, Yang M, Wang T, Wang N, Lyu L, Lam KY (2020) Local differential privacy-based federated learning for internet of things. IEEE Internet Things J 8(11):8836–8853

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