Multimedia Tools and Applications (2023) 82:25527–25558
https://doi.org/10.1007/s11042-022-14104-3

An efficient hidden marking approach for forensic and contents verification of digital images

Mohsen A. M. El-Bendary[1] · Osama S. Faragallah[2,3] · Sabry S. Nassar[4]

Received: 17 August 2021 / Revised: 19 October 2022 / Accepted: 25 October 2022 /
Published online: 13 January 2023

Abstract

Recently, forensic tools have been presented for detecting the forged image and illegal image manipulations. This paper presents an efficient and simple image contents verifying approach acting as a forensic technique. The presented approach mechanism is built by adding a hidden mark in a secret images, this mark achieves image integrity verification and detecting the tampering or forgery in the secret/authentic images. The secret/authentic/authentic image is divided to two main partitions, each portion is segmented to small blocks. These blocks in one partition are used to mark the blocks of the second partition using data transform technique. Firstly, the sensitive image is marked according to a self-embedding method. Then, a transform domain is utilized in order to embed a block-based signature into another block of the same image. Common discrete transform domains like DWT, DCT, and DFT are examined individually. Different analyses and comparison measurements are employed. The DCT is proved to be the most suitable and efficient transform domain to be used with the proposed scheme. At the receiver side, the reverse process is performed to verify image integrity. As proved from the experiments, this mark-algorithm is not visible or observable and robust against various attacks.

Keywords Data integrity · Hidden mark · Image verification · DCT · DWT · DFT · MSE · PSNR · Correlation · Image attacks

✉ Mohsen A. M. El-Bendary
engmohsen2004@yahoo.com

[1] Faculty of Technology and Education, Helwan University, Cairo, Egypt

[2] Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya 21974, Kingdom of Saudi Arabia

[3] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[4] Nuclear Research Center, Atomic Energy Authority of Egypt, Nasr City, Egypt

1 Introduction

Data integrity is one of the essential security requirements, it is the assurance that a sensitive data cannot be modified or accessed, and the only authorized persons do accessing or modifying in the classified data. In a highly sensitive applications such as; nuclear and military applications when the integrity of a related sensitive data is violated, a vital process may be disrupted as a consequence. For the reason of rapid advances in data processing techniques, the data content can be easily attacked, accessed and modified. Therefore, the capability of the integrity verification techniques should be focused on to be more sensitive to detect any unintentionally modifications (different noises added through transmission and unintentionally user misuse) or intentionally modifications (masquerade and forgeries). Digital watermarking methods are not only utilized for approving the owner identity, but also for protecting the multimedia content integrity.

The data forgery and image manipulation process, these issue are happened every day around the world. With increasing the amount of data transferring over the internet under the Internet of Things (IOT) or Cloud computing titles for different applications, this big amount of data need to protected from any manipulation and forgery. The level of the cyber crime will raise with the increasing data transferring. on the other hand, with the time, all people in different countries will depend on the internet. All these factors clears the need of a simple data contents protection approach. The rate of cyber crime around the world increases rapidly. That clears in the flow graphs of the cyber crime in the internet. So, the presented self-marked approach achieves the data contents protecting with a simple algorithm.

To verify image content integrity and detect various types of image forgery, different techniques have been emerged. These techniques should be capable of sensing any small image tampering and should be utilizable in many applications such as; law, journalism, national defense, etc. [7]. Image integrity could be verified using digital watermarking. Generally, watermarking technique embeds a message assigned as a watermark that's may be visible or invisible into an image, and then on the other hand the embedded watermark is extracted to verify the image content integrity. Traditional watermarking schemes require the receiver side to own the watermarks that are used by the sender to be compared with the extracted one as in [9, 49], which means that the watermark has to be created in a separate manner and transmitted in a secure route to a particular receiver which may compromise the security of the scheme.

Other common limitations of several watermarking schemes are; the necessity of the receiver to have a former knowledge about the transmitted image, i.e. image size, private keys, lookup table, etc. [14, 45]. Algorithms that depend on interrelationships among neighboring pixels during the watermarking process are not able to detect the cropping on the watermarked image [44]. Some algorithms require an extra processing overhead in watermark creation, embedding, extraction, and integrity verification, such as in [47]. In this method, the authors proposed an authentication and image integrity verification scheme using a public key cryptosystem and a content-based watermarks. On the transmission, a characteristic map of the underlying image is obtained as a watermark and then partitioned into blocks. A watermarked image to be created a neighboring feature map and watermark blocks are mixed and encrypted for embedding process. On the reception, the characteristic map is extracted from the obtained image and matched with the retrieved watermark to confirm the authenticity and integrity. This scheme is capable of detecting addition of foreign objects, removal of original objects, geometric transformation, identifying rigging, and cropping. Additionally, this public system does not need protected channel to deliver additional information like image dimensions and/or secret key. However, with RSA cryptosystem protection, it requires extra processing overheads in watermark extraction, embedding, and verification processes.

Also, the generality of previous efforts related to the same issues have concentrated on investigating methods under only the ideal case of noise-free channel [8, 35]. These methods are not practical when utilized to transmit sensitive images over the error-prone (noisy) wireless channel. Subsequently, there are a number of solutions that have been proposed for verifying image authentication in random packet loss existence case [46]. However, they often have a higher computational complexity, so their application in mobile communication may become critical, where the signature scheme should be efficient enough to verify authentication without any extra delays. The authors in [40] tried to overcome the security and data transmission constraints imposed by the wireless medium by proposing a signature-based image authentication technique. Although it tries to balance between the security and robustness, but a higher processing capability is still required.

The literature introduced many techniques [4, 5, 8, 12, 20, 23, 24, 27, 29, 35, 40, 44, 46, 47] that have critical problems with watermark verification, extraction and complexity considerations. They have low robustness and imperceptibility, i.e., in the presence of multimedia attacks, they failed in achieving adequate watermark and in extracting watermark subjective and objective qualities. Furthermore, in watermark embedding process, they failed in picking the most suitable regions inside the images. Thus, they increase the computations as well as effecting the quality and imperceptibility of the watermarked images. Considering the limitations of the state-of-the-art image integrity and verification watermarking techniques, this paper presents an efficient and secure image integrity and verification communication system to preserve both robustness and imperceptibility. Moreover, compared to the traditional image integrity and verification watermarking techniques, the proposed work has minimal computational overhead, high quality, high robustness, good imperceptibility, and sufficient resistance to most forms of multimedia attacks [2, 3, 6, 41–43, 48, 52].

It is know that the machine learning based is an approach for image classification [16, 26, 35]. It is also, employed as a method for verifying the data contents [22]. In [22], authors presented image forgery approach based on the Support Vector Machine (SVM). The social media security attacked the focusing of several researchers [17, 25, 50]. Really, it is very essential research point. In [50], Image authentication approach on the social media has been proposed based on the deep learning concepts utilizing the neural network. The presented approach in this research paper can be more efficient and acceptance for applicability and lower complex than the other approaches. The deep learning based approach utilizing for the data contents verification works according to two partition, the training and learning (feature extraction), the second partition is the classification process. On the other hand, the dependable approach for data verification is presented in this research paper, it is evaluated with presence the different attacks for measuring its stability and applicability. The presented approach aims to verify the image contents by put invisible mark to the image, this mark is very small of piece from image replaced by other piece with considering this mark is not observable. The decryption process here means verifying the contents of marked image. If there is no manipulation, the algorithm passes the verification process or if there is any littlie change (1 bit) or more, the verification process will detect this change and its place with high accuracy. Also, the reliability of this approach has been studied with presence the different attacks.

1.1 Contribution

In this section, our contribution in this research paper has been presented. Simple algorithm with lower complexity is proposed for achieving sufficient integrity of image contents. This algorithm is built based on data transform tools for hiding mark within the secret/authentic images. Utilizing this algorithm in the contents verification process provides capability for detecting any tiny tampering or forgery in the images due to any effects or attacks. Various data transforms techniques has been tested for choosing the suitable tool for performing the algorithm. Also, this research paper presents brief analytical describing of image processing steps and various format for executing the presented algorithm on the secret/authentic images.

This paper presents an approach for protecting and verifying integrity of image data content by exploiting one of the most popular transform domain techniques. The following sections will present in detail the proposed scheme and evaluate its performance in different situations of image integrity violations. The arrangement of the remnant of this paper is as follows. Section 2 gives a briefing review on DCT. Section 3 provides a systematic description of the proposed scheme. Then, the results analysis, comparisons, and the advantages and applications of proposed approach are presented and explained in section 4. Finally, Section 5 concludes this paper.

2 The discrete cosine transform

A Discrete Cosine Transform (DCT) generally can express a dedicated information point series like a summation of cosine functions oscillating at various frequencies. The 2D DCT is the most common category of DCT, which often used in signal and image processing [29]. The DCT when used with image data separates it into high, middle, and low frequency parts (FH, FM, and FL) as presented in Fig. 1. In low frequency component, much of the signal energy is located that includes significant visual portions of an image. In the other side, high frequency components are usually removed through compression. Therefore, a mid-band frequency is chosen for the use in watermarking. In this case, the watermark cannot be removed by compression and the embedding process will not alter the image visibility [19].

Eq. (1) gives the general formula of 2D transform of DCT for (NxM) image, it is formulated as follows [15]:

$$F_{(u,v)} = \left(\frac{2}{N}\right)^{\frac{1}{2}}\left(\frac{2}{M}\right)^{\frac{1}{2}}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right]cos\left[\frac{\pi.u}{2.M}(2j+1)\right].f(i,j)(1)$$

where v, u = 0, 1, 2…., N-1.

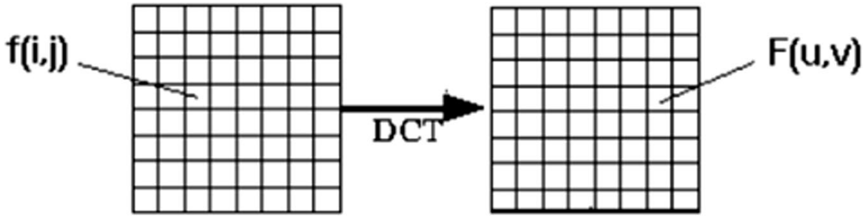


Fig. 1 DCT Transform: spatial domain to frequency domain

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

The parameters of Eq. (1) is presented as follows:- N and M represent image dimensions, rows and columns, respectively. Symbol *f(i, j)* represents the pixels intensity for pixel *P(i, j), F(u, v)* refers to the coefficients of DCT transform of pixel *P*(k_1, k_2)*.* The DCT transform contains three bands of frequencies, low frequency (LF) in upper left corner in the DCT coefficient matrix, medium frequency (MF) and high frequency (HF) which lies in low right location in DCT coefficient matrix. The DCT separates the image into parts of different frequencies and the top left coefficients correlate to low frequencies of authentic image block which the human eye is more sensitive to their changes, and as we move away from top-left corner in all directions, the DCT coefficients correlate to higher frequencies of authentic image block which the human eye is less sensitive to their changes, so they can be discarded in compression process, and hence this concept is basically exploited in the construction of the proposed integrity verification algorithm which the changes in the last bottom row, and the last right column for each image block does not affect the image visibility significantly.

3 Verification algorithm description

The model investigated in this work can be considered as a multi-task scheme that can be used for confidential image integrity verification. It is considered self watermarking algorithm without cover need. There are several research papers proposed image security techniques [10, 11, 21, 51]. These presented techniques in the previous research work tried to develop the traditional image security tools which are the encryption or the hiding through the watermarking or the steganography [1, 28, 37]. The main contribution of the proposed work that it tries to avoid most of popular limitations in traditional watermarking techniques and can be characterized by:

- Content-based watermarking in which watermark depends on the authentic image.
- No need for an additional secure communication channel to send an extra information concerning to authentic sensitive image.
- Providing a higher modification sensitivity to detect any small manipulation even it was imperceptible.
- Applicable to detect the tamper regions in the forgery marked images.
- Suitable for image confidence verification, which means that it can efficiently differentiate between received marked and non-marked image.
- Applicable to be applied on a wireless channel at different noise levels.
- It has an acceptable applicability to verify the integrity of an encrypted version of the image, so a higher security level can be obtained (confidentiality and integrity achieved at the same time).

The proposed model consists of two sub-models. The first sub-model implements the embedding process while the second one implements the verification process. Figure 2 describes briefly the proposed algorithm where an input secret image is marked using embedding process. The marked image is possibly manipulated through distribution by different

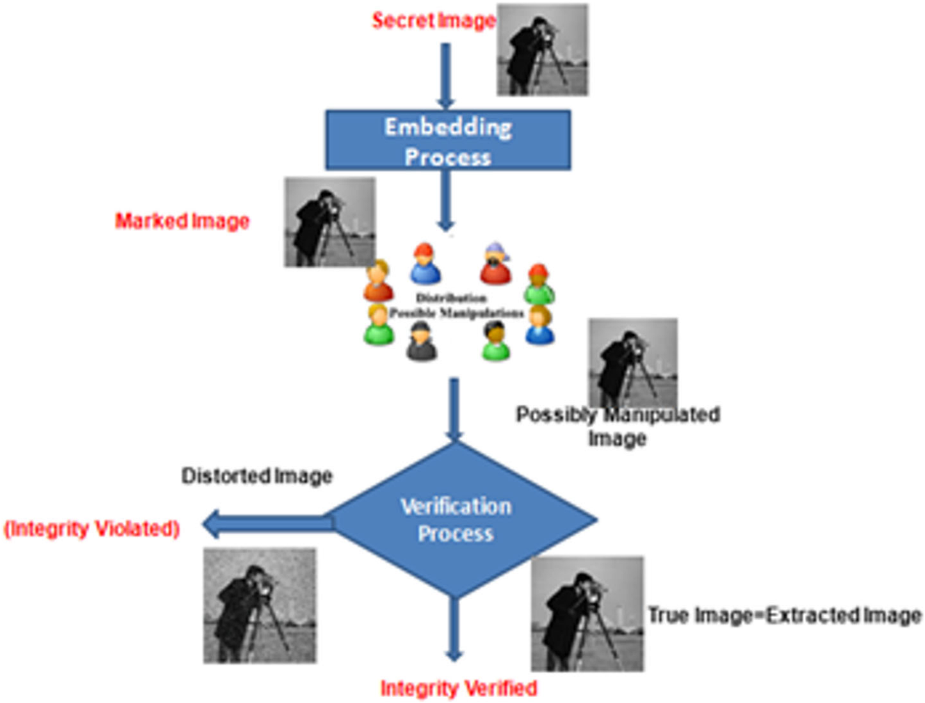


Fig. 2 Image integrity verification model

manipulation reasons and intentions. On the other side when a marked (possibly manipulated) image is received, it will be subjected to a verification process which acts as a decision-making process. If the received image is safely distributed (not manipulated), the output of verification process will be a truly extracted copy of an authentic image and its integrity is verified, otherwise the verification process output will be a distorted image. The visual properties and statistical analysis will tend directly to the amount of modification which the marked image is subjected on the distribution process.

The two models are explained in sections 3.1 and 3.2. In addition, to determine which one of the three commonly used frequency domain transforms (DWT, DCT, and DFT) is more applicable to be used in the proposed model, a comparison among those transforms has been introduced with respect to having acceptable image analysis results.

In the following: simple mathematical represents the presented algorithm, where secret/authentic image is represented in a matrix within different format.

– Mathematical Expression

In the following, a simple mathematical model of the image segmentation in the mark-embedding algorithm is presented. Firstly, the algorithm is built based on the self mirror concept, two equals partitions work as a mirror together. In Eq. (2), the original data is represented as a matrix, it dimensions are (MxN), and it’s elements are given in Eq. (3).

$$F = I(MxN) \qquad \text{where}, M \neq N \tag{2}$$

$$F(M,N) = \begin{bmatrix} a_{(1,1)} & a_{(1,2)} & \cdots & \cdots & a_{(1,N-1)} & a_{(1,N)} \\ a_{(2,1)} & a_{(2,2)} & \cdots & \cdots & a_{(2,y)} & a_{(2,y)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(M,1)} & a_{(M,2)} & \cdots & \cdots & a_{(M,N-1)} & a_{(M,N)} \end{bmatrix} \tag{3}$$

The data matrix F is converted to square matrix as in Eqs. (4) and (5), the data form in Eq. (3) is formatted to square form, it' dimensions (YxY).

$$F_{\text{square}} = I_S(YxY) \tag{4}$$

$$F_{\text{Square}}(y,y) = \begin{bmatrix} a_{(1,1)} & a_{(1,2)} & \cdots & \cdots & a_{(1,y-1)} & a_{(1,y)} \\ a_{(2,1)} & a_{(2,2)} & \cdots & \cdots & a_{(2,y)} & a_{(2,y)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(y,1)} & a_{(y,2)} & \cdots & \cdots & a_{(y,y-1)} & a_{(y,y)} \end{bmatrix} \tag{5}$$

The image is segmented to two equal partitions, up and down partitions, as given in Eq. (5) (The) $F_{\text{Square}}(y,\ y)$ is divided to equal partitions as shown in Eq. (5) : −

$$F_{\text{Square}}(y,y) = \begin{bmatrix} P1P_{\text{up}}(y/2,y) \\ P2_{\text{Down}}(y/2,y) \end{bmatrix} \tag{6}$$

The elements of the processed image in the square matrix form are formulated in Eq. (6) as follows:

$$F_{\text{Square}}(y,y) = \begin{bmatrix} a_{(1,1)} & a_{(1,2)} & \cdots & \cdots & a_{(1,y-1)} & a_{(1,y)} \\ a_{(2,1)} & a_{(2,2)} & \cdots & \cdots & a_{(2,y)} & a_{(2,y)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{(y,1)} & a_{(y,2)} & \cdots & \cdots & a_{(y,y-1)} & a_{(y,y)} \end{bmatrix} \tag{7}$$

The second step is square image dividing to two partition, Eq. (7) represents the square matrix with considering the segmentation process, as shown in this Eq. (8), there are another variable is appeared (β), this symbol equals the small blocks size as mentioned in the previous section.

$$F_{\text{Square}}(y,y) = \begin{bmatrix} a_{((i-1)x\beta+1,(j-1)x\beta+1)} & a_{((i-1)x\beta+1,(j-1)x\beta+1)} & \cdots & \cdots & a_{((i-1)x\beta+1,(j-1)x\beta+y)} \\ a_{((i-1)x\beta+2,(j-1)x\beta+1)} & a_{((i-1)x\beta+2,(j-1)x\beta+2)} & \cdots & \cdots & a_{((i-1)x\beta+1,(j-1)x\beta+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{((i-1)x\beta+y,(j-1)x\beta+1)} & a_{((i-1)x4+N,(j-1)x4+2)} & \cdots & \cdots & a_{((i-1)x\beta+y,(j-1)x\beta+y)} \end{bmatrix} \tag{8}$$

The symbol β denotes to the size of small blocks, it proves the flexibility of this algorithm, it can be executed employing the different β values, β = 4 means the blocks size is 4 × 4 matrix, β = 8 means the blocks size is 8 × 8 matrix and β = 16 means the blocks size is 16 × 16 matrixes and etc. The symbol β can be employed in the combined different security levels. The every block can be encrypted individually utilizing the different secret key, where the secret key length is determined based on the size of the encrypted matrix. The encryption process merging in the marking embedding algorithm is considered additional feature in this presented work. Moreover, there are two approaches for the merging process, the marked image encryption approach, in this approach, the mark embedding process is followed by the encryption to produce the combined multi-levels of security. The second approach is the marking of the encrypted image, this approach starts with the encryption process, this encrypted image represents the input image of the algorithm for producing the marked encrypted image. The suitability of these two approaches is determined according to the level of the image sensitivity and its contents importance. I.

In Eq. (9) example for the processed image segmentation to small equal blocks in case of $\beta = 8$.

$$F_{\mathrm{Square}}(y, y) = \begin{bmatrix} a_{((i-1)x8+1,(j-1)x8+1)} & a_{((i-1)x8+1,(j-1)x8+1)} & \cdots & \cdots & a_{((i-1)x8+1,(j-1)x8+y)} \\ a_{((i-1)x8+2,(j-1)x8+1)} & a_{((i-1)x8+2,(j-1)x8+2)} & \cdots & \cdots & a_{((i-1)x8+1,(j-1)x8+1)} \\ \vdots & \vdots & \vdots \quad \vdots & \vdots \quad \vdots & \vdots \\ a_{((i-1)x8+y,(j-1)x8+1)} & a_{((i-1)x8+N,(j-1)x8+2)} & \cdots & \cdots & a_{((i-1)x\beta+y,(j-1)x8+y)} \end{bmatrix} \tag{9}$$

In Fig. 3, the mirror concept is applied on the square matrix as shown. There are several options for the mirror applying as shown in Fig.1a–e. As shown in this figure, there are four styles can be used for Segmenting the data square matrix form to two equal partitions, These styles are denoted by M_1, M_2, M_3 and M_4. In every style, the two partitions are segmented to equal small blocks, as the two partitions have the same size, the blocks in each partition contains the same number of blocks and the same size. In the following: the simple mathematical equations have been presented to formulate these four styles.

The style M_1 and M_3 are known by the ordinary styles, they can be expressed mathematically in simple form. On the other hand, the styles M_2 and M_4 are not applicable for the images processing, it may accepted and applicable for the audio or text information. In general, the mathematical model of these styles is discussed and presented. The presented mathematical model of the data contents verifications integrity must be invisible and not observable by the human eyes, this is the only condition for the applicability in the real applications for the recorded/archived multimedia information or for the image, audio, video, and text transmission over the different wireless noisy channels. Figure 3b is the used style in this presented algorithm.

In our presented research paper, the style M_1 is considered in the presented approach for achieving the image contents verifications against any forgery of illegal manipulation. For enhancing the security and confidentiality of the presented approach the style models “M_2, M_3 and M_4” can be utilized for marking the secret/authentic/authentic images. As shown in Fig. 3, styles M_3 and M_4 are complex more than styles M_1 and M_2.

3.1 Embedding process

This section presents how to mark highly sensitive image data that may be archived for a dedicated use or transmitted over untrusted communication medium. This embedding process takes a confidential image, as an input, and produces a signed block-based image (Marked Image), as an output. Utilizing a standard gray scale image as the authentic image, the

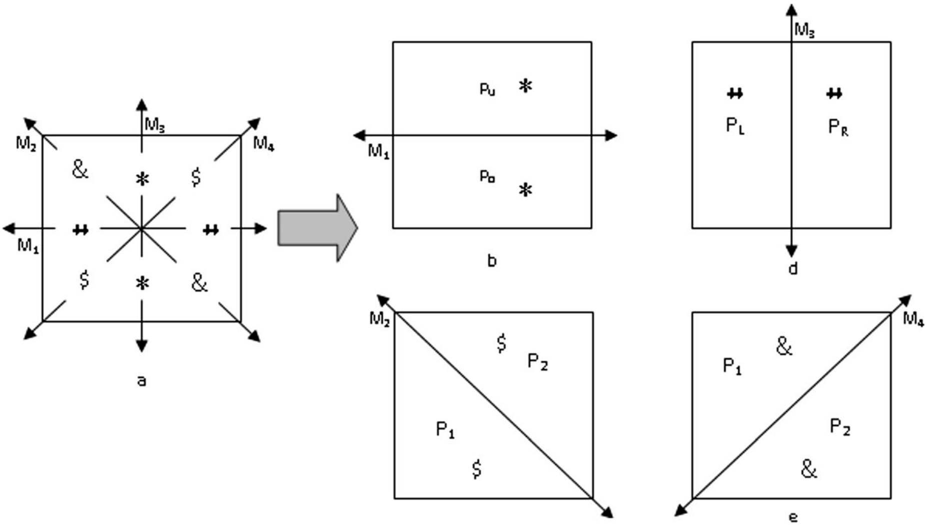


Fig. 3 The different segmentation styles of the processed data in square matrix form, a. Original square matrix form, b-M_1 style, c-M_2 style, d-M_3 style, e-M_4 style

embedding process is described briefly in the block diagram shown in Fig. 4 is depicted in stepwise as follows:

1- The authentic image *f* is divided into two equal parts *f*1 (Upper partition) and *f*2 (Lower Partition), where the dimension of (*f*1)partition = the dimensions of the (*f*2) partition. Then, each part is divided into equal number of 8 × 8 non-overlapping small blocks of pixels. That means the number of small blocks is the same in the two image partitions (*f1* and *f2*).
2- Apply the Transform Data (TD) for each block starting from left to right and from top to bottom through *f*1.
3- Working with *f*2 from left to right, top to bottom, row *k*; (*k* = 1, 2, 3, …, 8), and column *k* of block (*s*) are inserted as a replacement for row *k*, and column *k* of the transformed blocks in the similar place (*s*) across *f*1, where *s* = 1, 2, 3, ….., *M* × *N*/128, in case of authentic image of size (256 × 256), when divided into two equal parts (*f*1, *f*2) their sizes will be (128 × 256), every part is then divided to non-intersecting blocks of size 8 × 8, so the amount of blocks per one part of image will be; (*s*) = (128 × 256)/(8 × 8) = (512).
4- Apply the inverse TD for each block starting from left to right and top to bottom through *f*1.
5- Repeat step 2 and 3, for every block in *f*2, and row *k*, column *k* of the original (*f*1) blocks are inserted instead of row *k*, and column *k* of the altered blocks in the same order (*s*) via *f*2.
6- Apply the reverse TD for each block of *f*2.
7- Assemble the two parts of the image to obtain a block based marked image (*x*).

The operation mechanism of the marking process can be briefed as follows: firstly, the processed image is divided to upper and lower partition, these two partition equal in the dimensions. Also, the number of blocks in partition f1 equals the blocks in the partition f2. The partitions f1and f2 form the image, these partitions are processed together. The image always is one piece, But, the marked image will generated from the original one by replacing the very

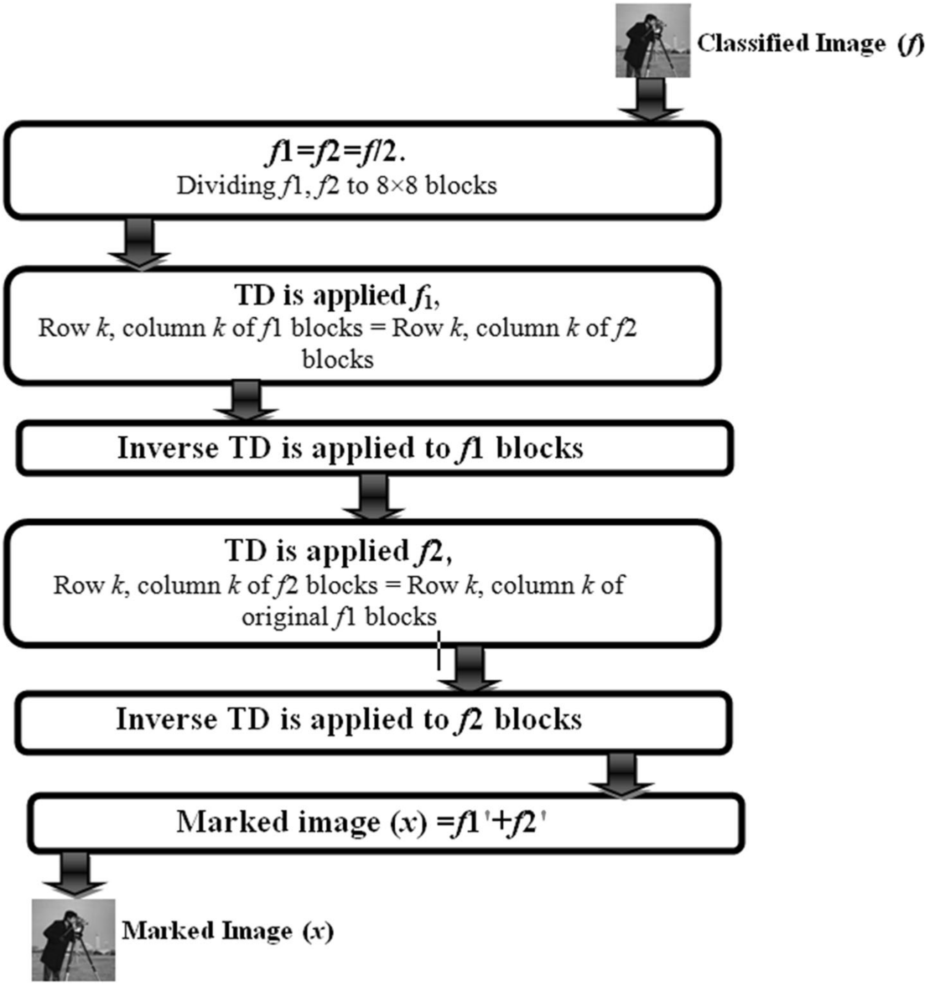

Classified Image (*f*)
*f*1=*f*2=*f*/2.
Dividing *f*1, *f*2 to 8×8 blocks
TD is applied *f*1,
Row *k*, column *k* of *f*1 blocks = Row *k*, column *k* of *f*2 blocks
Inverse TD is applied to *f*1 blocks
TD is applied *f*2,
Row *k*, column *k* of *f*2 blocks = Row *k*, column *k* of original *f*1 blocks
Inverse TD is applied to *f*2 blocks
Marked image (*x*) =*f*1'+*f*2'
Marked Image (*x*)

Fig. 4 The proposed embedding process. Notes: the original block of the partition *f1* is transformed by DCT and the block of partition *f2* is also, transformed by the DCT. Hence the replacement is happened in the transformed version. After that, the marked block retransformed to the data/pixels form by IDCT and put in the new position

small piece of image from f1 by very small piece of image to f2 and verse versa through the data transforming tool.

3.2 Verification process

This model implements the reverse process of the embedding scenario. It takes the marked image as an input and reconstructs the true authentic image in case of no modification occurs through distribution. Figure 5 and the following steps describe the flow of extraction process with a DCT as an efficient TD used with embedding process which will be shown clearly in the comparison results in the following sections:

1- Input the marked image.

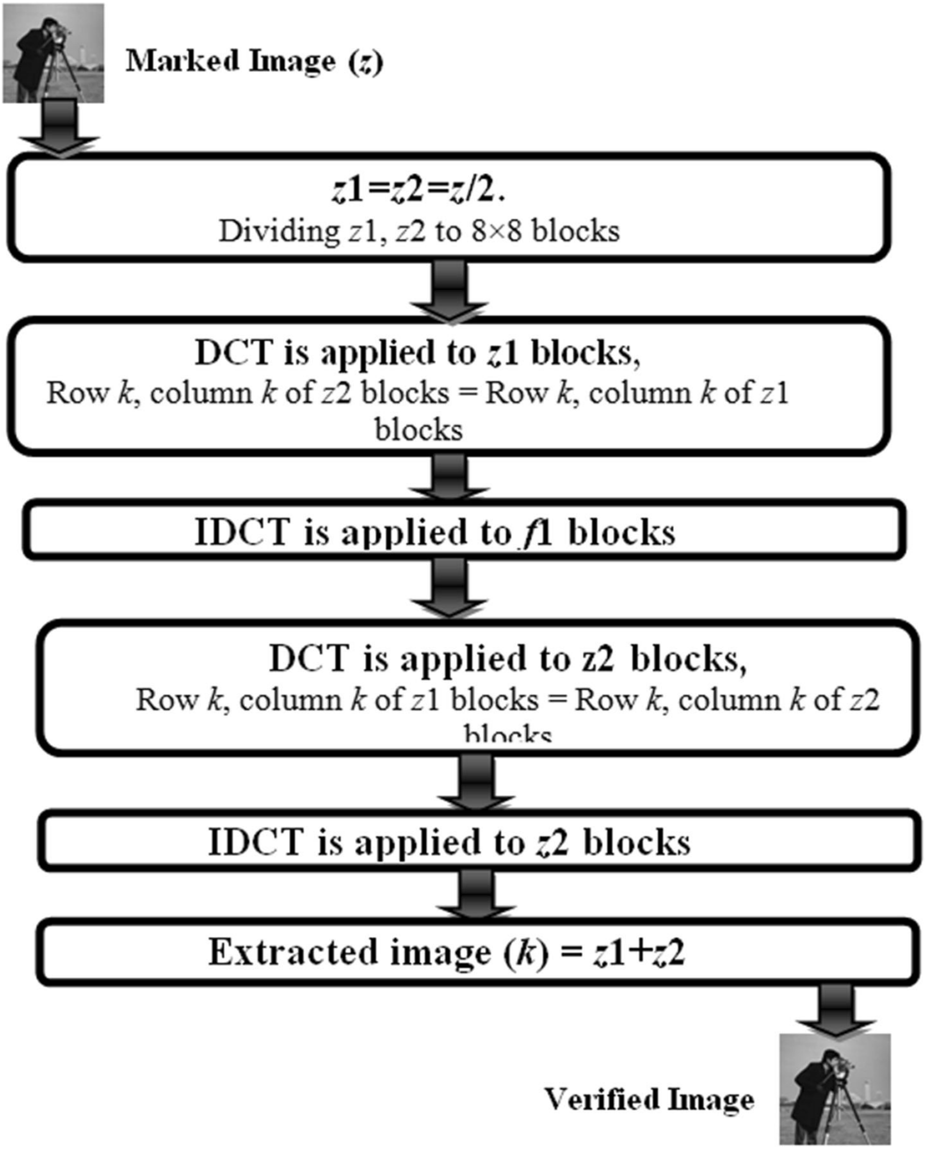
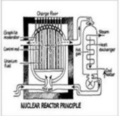
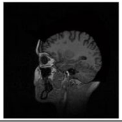
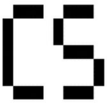

Marked Image (z)
z1=z2=z/2.
Dividing z1, z2 to 8×8 blocks
DCT is applied to z1 blocks,
Row k, column k of z2 blocks = Row k, column k of z1 blocks
IDCT is applied to f1 blocks
DCT is applied to z2 blocks,
Row k, column k of z1 blocks = Row k, column k of z2 blocks
IDCT is applied to z2 blocks
Extracted image (k) = z1+z2
Verified Image

Fig. 5 The proposed verification process

2- The observed image (z) is divided into two identical parts $z1$ and $z2$, where $z1 = z2$. Then, each part is divided to 8 × 8 non-overlapping blocks of pixels.
3- Apply the DCT for each block starting from left to right and top to bottom through $z1$.
4- Row k and column k of transformed $z1$ blocks are inserted instead of row k, and column k of the blocks in the same place (s) via $z2$.
5- Apply the reverse DCT to every block through $z1$.
6- Repeat steps 3 and 4, but for every block of the original $z2$, and row k, column k of transformed $z2$ blocks are inserted instead of row k, and column k of the blocks in the same place (s) via the original $z1$.

Table 1 Different samples of authentic images

Name	Cameraman	Lena	Reactor Principle	Medical Image	Copyright	Boy
Image						

7- Apply the inverse DCT for each block of *z*2.

8- Assemble the two parts of the image to obtain an extracted image in case of no modification occurred.

4 Results analysis and comparative study

MATLAB R2018a with windows7 environment were utilized to establish simulation experiments. The performance of the proposed model was evaluated in case of popular transform domains. In DFT case, the pervious steps are almost implemented. However, in DWT case, a 2-level Haar DWT is utilized to every block that results in the creation of the four bands, i.e. HH1, LH1, HL1, and LL, with size (4 × 4). The LL band is chosen for inserting a mark of the same order block in the second part of the image. All tests were applied on various benchmark gray scale images with size of (256 × 256) as an authentic image, which are presented in Table 1. These images are used for testing the applicability and validity of the presented algorithm. The testing images contain standard Matlab images and X-ray image (medical image), it is not standards image, real image (reactor image) is not standards image for representing the variety in the testing process.

4.1 Evaluation of embedding process

Quality metrics are utilized to evaluate the performance analysis of the proposed scheme. These quality metrics are calculated and discussed for every transform domain individually to determine which transform domain is more suitable and efficient for using with the proposed algorithm.

4.1.1 The image histogram analysis

Histogram is widely used as a metric for image encryption/decryption technique [32]. In general, Histogram is considered a visual graph presentation for summarizing the data/image and it represents the frequency graph of numerical data by rectangles graph. The origin of "Histogram" term is given from "Histos", which is Greek word means pole/g (chart-graph). The quality of image encryption is indicated by the Histogram, flat graph means ideal encrypted image and efficient encryption algorithm. Therefore, the Histogram of encrypted image can be considered one of the most methods to clear the quality of image encryption technique.

Histogram graph provides the comparative number of occurrences of each pixel through an image and considered as one of the most important methods for the evaluation of the quality of an image. Authentic image and marked image (output of embedding process) with their histograms for every transform domain with two different images (Cameraman and Reactor design) are shown in Figs. 6, 7, 8, 9, 10 and 11, respectively. In this research paper, the Histogram is utilized for ensuring the invisibility/ not observable mark of the presented algorithm.

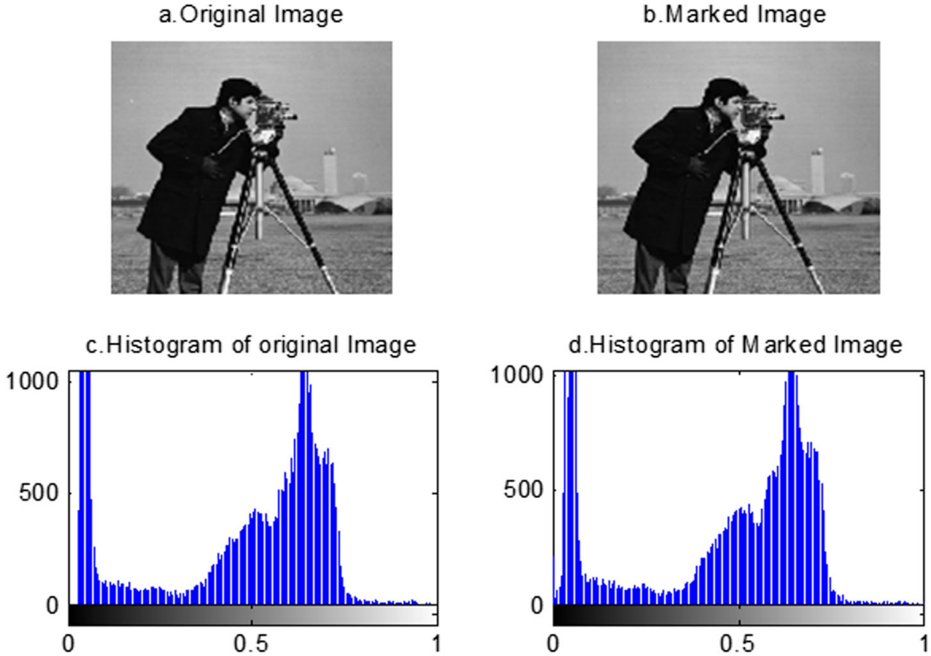


Fig. 6 Authentic image, Marked image, and their histogram in case of DCT (Cameraman)

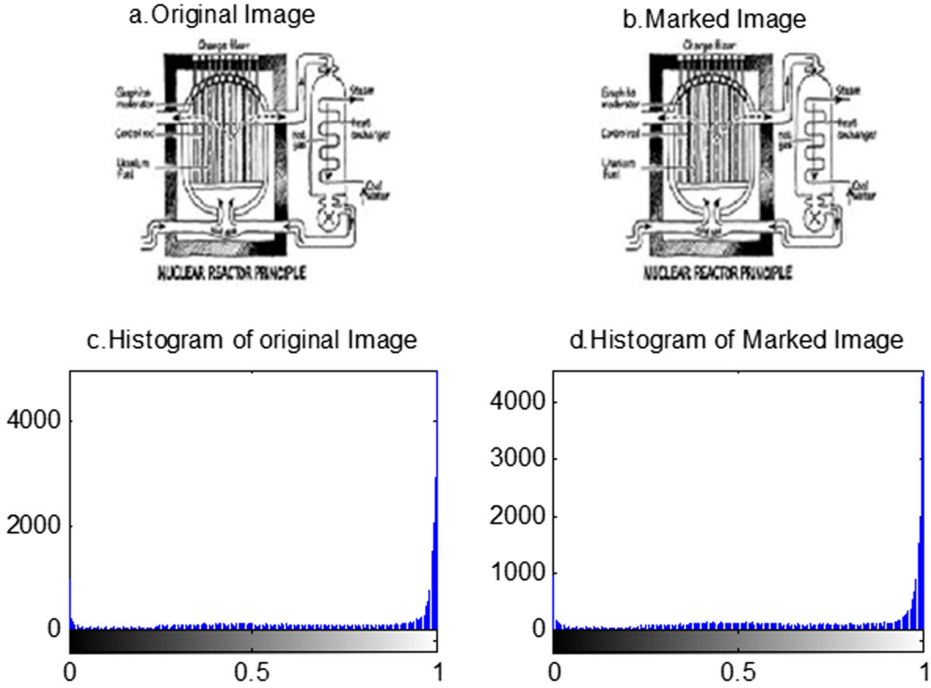


Fig. 7 Authentic image, Marked image, and their histogram in case of DCT (Reactor design)

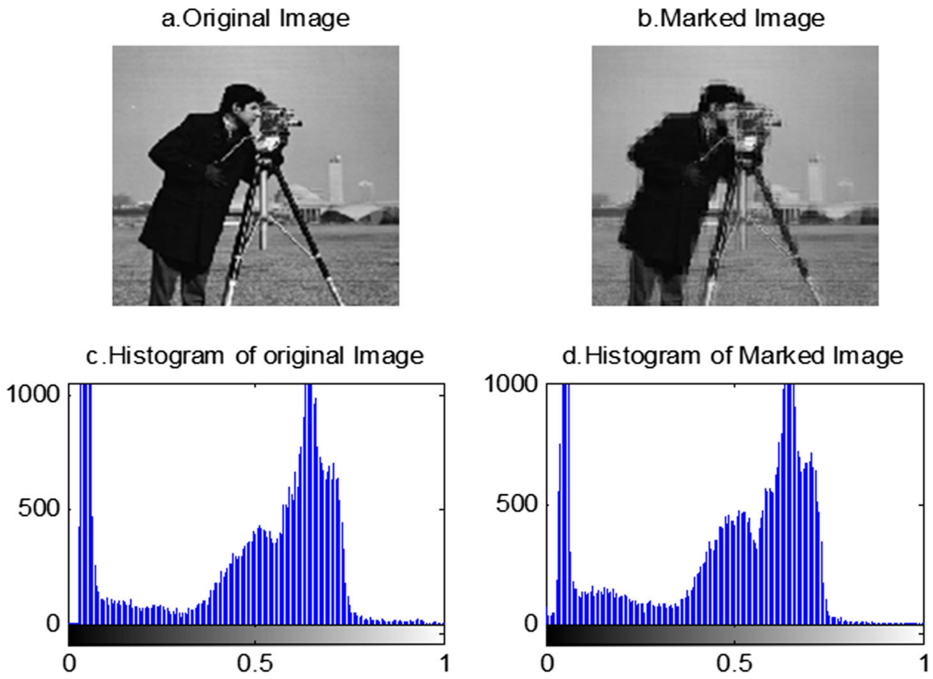


Fig. 8 Authentic image, Marked image, and their histogram in case of DFT (Cameraman)

The results indicate that when the proposed algorithm is implemented using DCT, the two images, i.e. authentic and marked, appear to be the same and their histograms are approximately the same. Thus the results verifies that utilizing DCT produces the most acceptable results related to imperceptibility and image histogram analysis.

4.1.2 Correlation (C_r)

It is a measure that is utilized to evaluate the degree of closeness between the two functions, it can be used to determine the extent to which two images are remained close to each other. The correlation ratio gives a direct measure of the efficiency of the proposed algorithm. The closer the correlation ratio to unity, the efficient the algorithm [48].

4.1.3 Mean square error (MSE)

MSE is the median measure of the squares of the difference between the intensities of two examined images. It can be mathematically represented by Eq. (10).

$$MSE = \frac{1}{MxN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(f(i,j) - f^{'}(i,j) \right)^{2} \qquad (10)$$

where $f(i, j)$ and $f'(i, j)$ are assigned for the authentic and marked images respectively. The higher the value of MSE, the lower the quality of the image and vice versa [34].

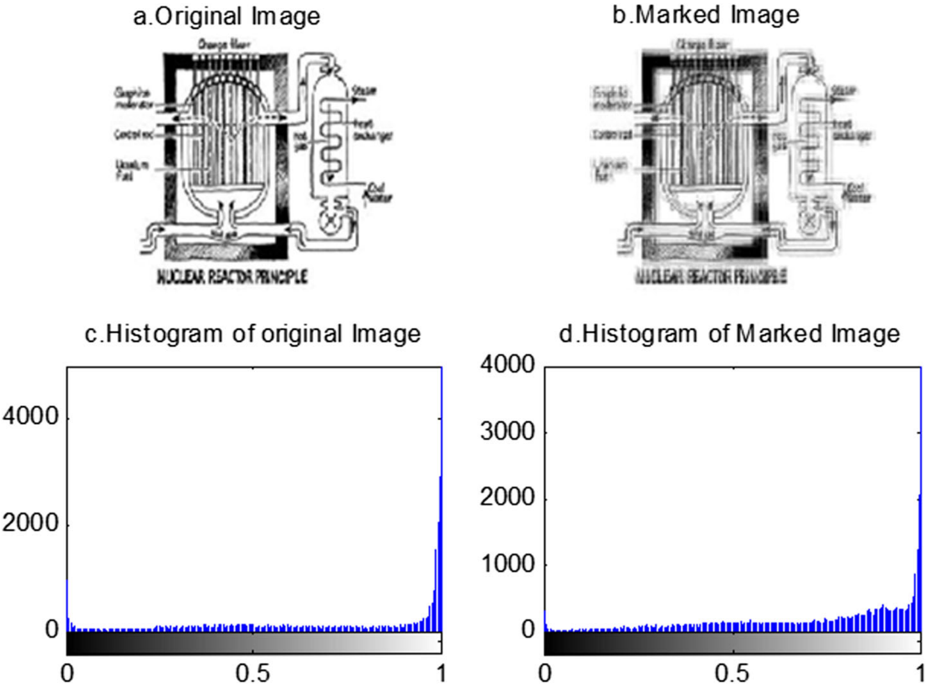


Fig. 9 Authentic image, Marked image, and their histogram in case of DFT (Reactor design)

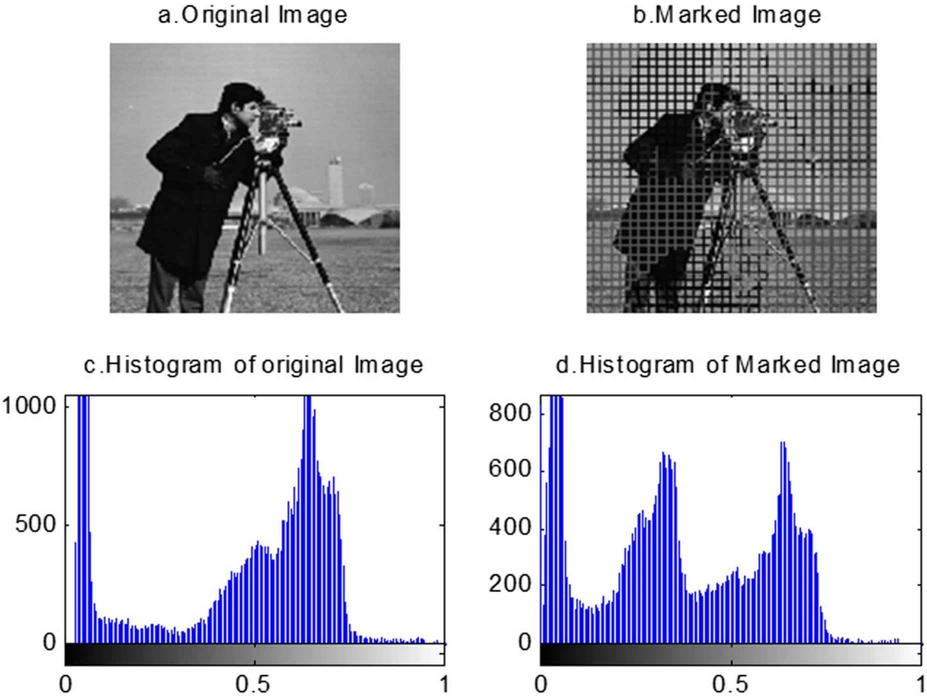


Fig. 10 Authentic image, Marked image, and their histogram in case of DWT (Cameraman)

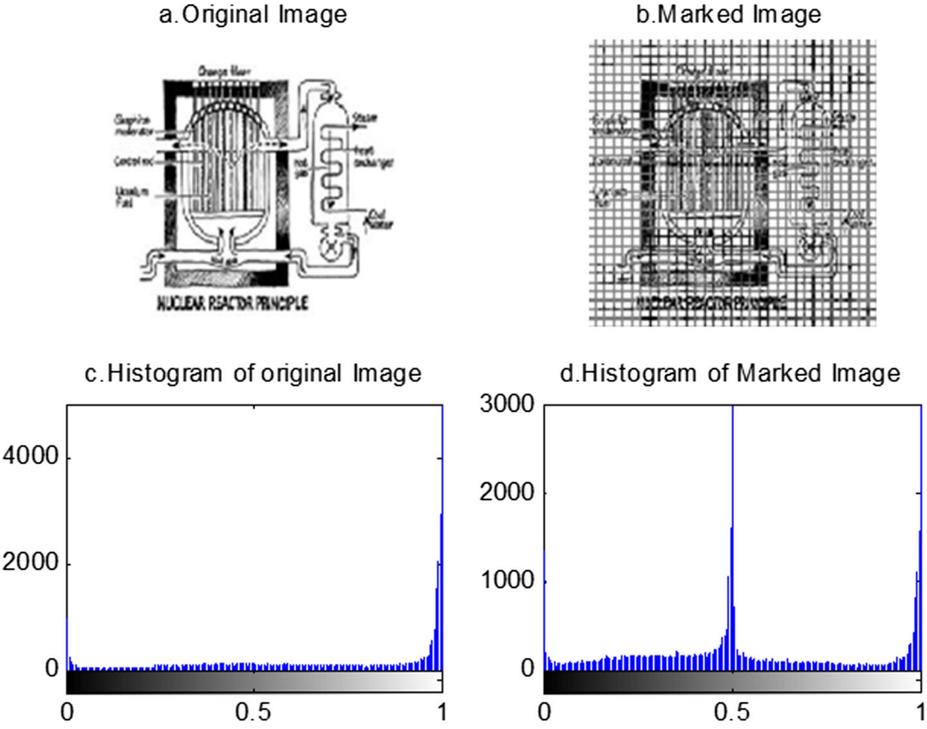


Fig. 11 Authentic image, Marked image, and their histogram in case of DWT (Reactor design)

4.1.4 Peak signal-to-noise ratio (PSNR)

The PSNR is an image quality metric used for differentiating between two examined images. It can be formulated mathematically in Eq. (11). A higher value of PSNR is an optimum case [34].

$$PSNR(dB) = 10\log\left(\frac{255^2}{MSE}\right) \tag{11}$$

The PSNR, MSE, and correlation are computed for the three utilized transform domains with two different images (Cameraman and Reactor) and are utilized for testing the presented technique for contents verifications through the computer experiments.

Table 2 Quality metrics for marked image using various transform domains

Transform Domain	Image Quality Metrics					
	MSE		PSNR		C_r	
	Cameraman	Reactor	Cameraman	Reactor	Cameraman	Reactor
DCT	19.07	7.25	35.32	29.50	0.997	0.993
DFT	35.09	12.15	32.78	27.30	0.9781	0.952
DWT	36.03	17.45	12.54	9.50	0.6060	0.588

The results of these initial experiments are listed in Table 2 and the images samples with the Histogram of the original and marked images have been shown in Figs. 6, 7, 8, 9, 10 and 11. Higher PSNR, lower MSE, and higher correlation ratio are acquired in case of realizing the proposed system using DCT, which the replaced rows and columns through the algorithm procedure are selected to be the eighth row, and eighth column ($k = 8$) for each block of size (8×8).

As shown in the images samples of the results in Figs. 6 and 7 for cameraman and reactor, respectively. The marking of contents is not visible, the original and marked image appear as the same. Also, there is no difference in the Histogram of the authentic and marked images. Figures 6 and 7 show the results of image verification based on DCT transform. Figures 8, 9, 10 and 11 give the results of the algorithm based on DFT and DWT transform techniques.

The Original authentic image and marked cameraman image are given in Fig. 6a and b, respectively. As cleared form these images, the mark don't affects on the image and it is not observable by human eye. Figure 5c and d show the Histogram of original and marked cameraman image, there is little difference between them.

DCT-based algorithm achieves better than other scenarios. The Original authentic image and marked Reactor image are given in Fig. 7a and b, respectively. As cleared form these images, the mark don't affects on the image and it is not observable by human eye. Figure 7c and d show the Histogram of original and marked cameraman image, there is little difference between them.

The image content verification algorithm based on DFT and DWT testing experiment have been given in Figs. 8, 9, 10 and 11. As shown in Fig. 8a and b, the mark is observable, the Histogram of authentic image and marked cameraman images illustrate the variations between the original and marked image versions. Figures 8c-d show the results of DFT using Reactor image.

The previous results of the different computer experiments reveal the suitability and applicability of the DCT-based image content verification algorithm more than the other data transform techniques due to invisibility of the mark. Figures 10 and 11 show results of DWT-based algorithm, it is cleared the difference in Histogram of original authentic and marked images. The results of the previous experiments have been tabulated in Table 2.

In the previous results samples, the block size is 8×8, it is chosen for testing the performance of different data transform techniques. In the next section, the performance of the various block size has been studied. As shown in the computer simulation experiment, the DCT transform performs better than the other techniques with the presented scenario of the simulation parameters as shown in Table 2.

4.2 Evaluation of embedding process

Assuming that no attacks tampered the marked image and the transmission medium is of free errors. The extraction process is implemented using DCT domain only as an efficient transform to be used with the proposed algorithm which achieved best performance results through embedding process. Figures 12 and 13 show the authentic image, extracted image, and their histograms for two different images. In case of no modification, the authentic image is extracted successfully, and image integrity is verified.

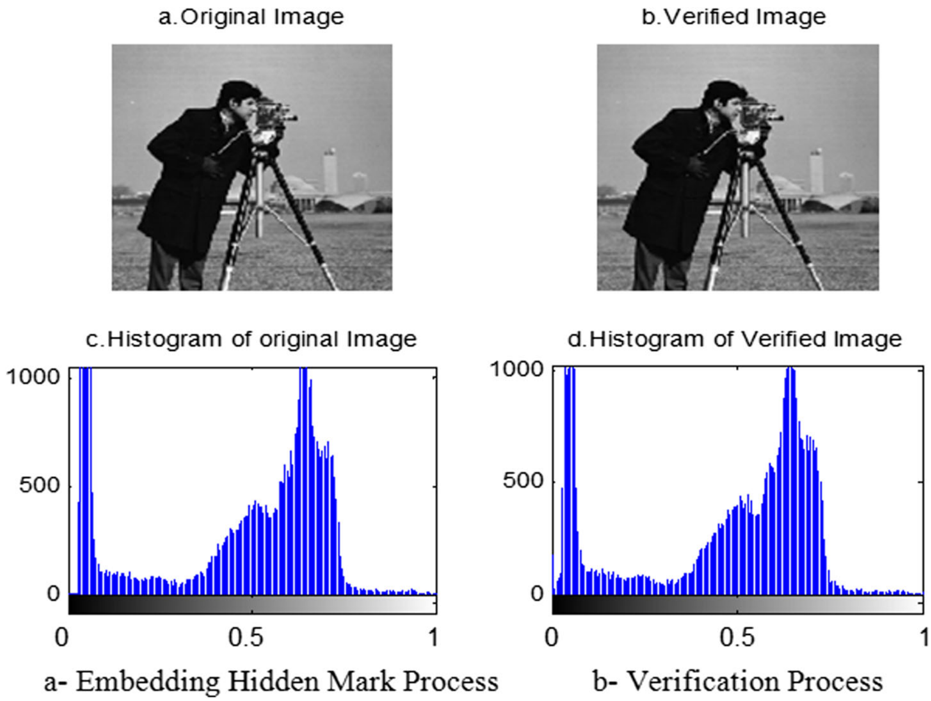


Fig. 12 Authentic image, Verified extracted image, and their histogram in case of DCT (Cameraman)

The image quality metrics are listed in Table 3. These metrics assure the acceptable efficiency of the proposed verification algorithm. Every block is exposed to DCT and its reverse with their standardized quantization, and at every time some error is introduced during quantization process. Therefore, a tiny variation in the correlation ratio between the authentic and obtained images is presented. For more evaluation of the proposed image integrity verification algorithm, its performance is evaluated at different block sizes. The algorithm behavior at block sizes of 4 × 4 and 16 × 16 is compared with its previously discussed behavior at 8 × 8 block size. The performance metrics (MSE, PSNR, and Cr) are measured and compared during embedding process between the authentic and marked images for the three assigned block sizes and introduced in Table 4. Also, these metrics are measured during the verification process between authentic and verified extracted image in case of no image manipulations and listed in Table 5. The results reveal that the best performance of the proposed system is achieved with a block of size 16 × 16. Hence, in the rest evaluating simulation experiments the size block is 16 × 16.

To examine the practicality of the proposed image integrity verification algorithm, it applied on different images with different visual properties. Table 6 shows the extracted verified image and related quality metrics between the authentic and extracted verified images which are measured individually for every image sample. The results reveal the sufficient applicability of the proposed algorithm to verify image integrity.

As shown in Figs. 14 and 15, the marked image appears as the original image. These figures show the various versions of the processed images. Firstly, Fig. 14 shows the results of standard Matlab (Cameraman image) for testing the visibility and delectability of the algorithm. Figure 14b gives the verified/extracted standard Cameraman image. The experiment

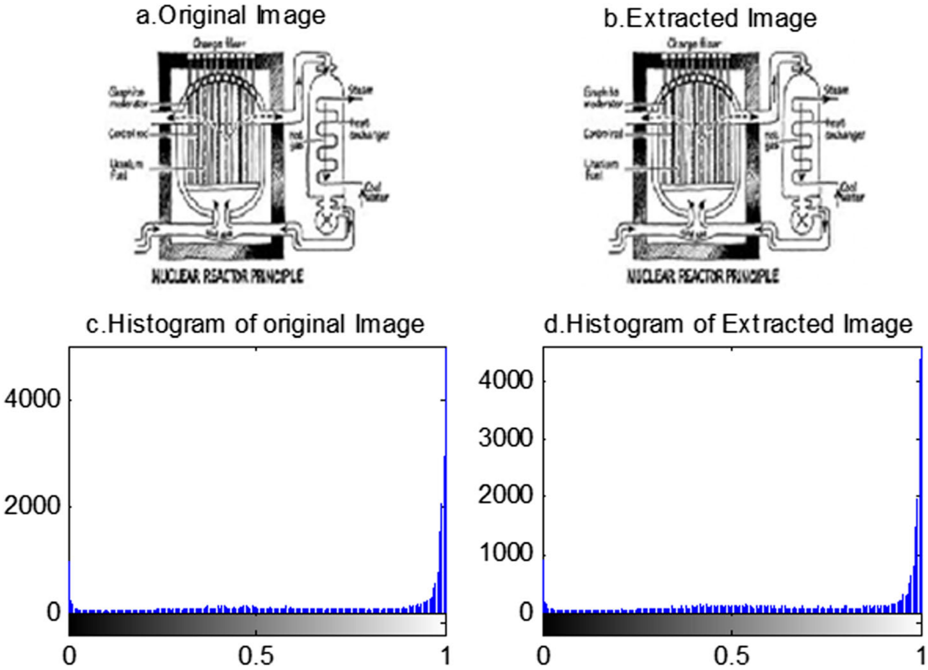


Fig. 13 Authentic image, Verified extracted image, and their histogram in DCT case (Reactor design)

repeated using the reactor image as not standard image. Figure 15a and b give the embedding hidden mark and verification processes images samples, respectively. As shown, in Fig. 15b, extracted/verified image appears like/same original image.

4.3 Advantages and applications

The following sections describe experimentally the advantages and some different applications of the proposed image content integrity verification approach.

4.3.1 Modification detection sensitivity

The detection sensitivity is considered a major aspect related to the integrity verification algorithm evaluation, which describes the ability of the algorithm to detect any small image manipulation even it was visibly undetectable. To achieve a comprehensive assessment of the proposed algorithm performance, the detection sensitivity analysis is built upon two aspects;

Table 3 Quality metrics of Image using DCT domain for block size 8 × 8

Transform Domain	Image Quality Metrics					
	MSE		PSNR		C_r	
	Cameraman	Reactor	Cameraman	Reactor	Cameraman	Reactor
DCT	16.63	62.40	36.05	30.20	0.998	0.994

Table 4 Performance metrics of marking process for different block sizes

Block Size	Image Quality Metrics					
	MSE		PSNR		C_r	
	Cameraman	Reactor	Cameraman	Reactor	Cameraman	Reactor
4×4	52.0	175.8	31	25.7	0.993	0.984
8×8	19.03	72.50	35.3682	29.5	0.997	0.993
16×16	8.50	31.10	38.84	33.2	0.999	0.997

a) Visual detection, which depends on the visual properties of the verification algorithm output image.

b) Statistical analysis, which depends on some measured parameters between the input and the output of the verification process.

The detection sensitivity analysis is focused on measuring the performance of the proposed algorithm to sense the visually undetectable manipulation attacks to highlight its importance. Because the most image manipulations which have a forensic nature are intended to be visually undetectable and the image receiver cannot visually detect the forensic act that is usually having a severe impact on the future or tampered image dependable issues. Visual detection is a method used to detect the image integrity violation, depending on the visual properties of integrity verification process for the output image. The quality of the output image is inversely proportional to the amount of modification occurred. The proposed scheme performance is studied in the case of two categories of manipulations;

a) Large scale and visually undetectable manipulation attacks, including; image resizing attack, image blurring attack, Gaussian noise, and salt & pepper noise.

b) Small scale and visually un-detectable manipulation attacks, including copy-move forgery, and sub-image blurring attack.

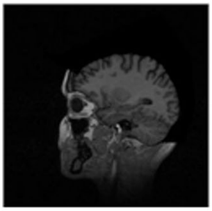
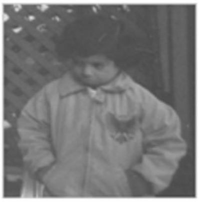
I. Large Scale and Visually Undetectable Image Manipulation Attacks

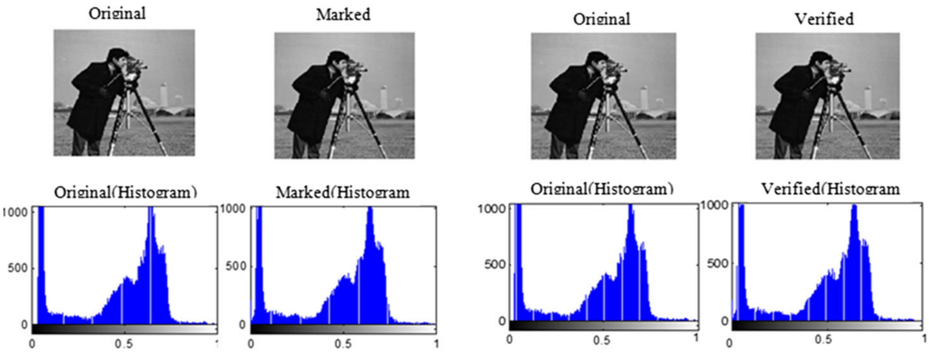
Large scale image manipulation attacks are those manipulations that affect a large relative area of an intended image. These modifications may be mainly for forgery intent, such an image resize, image blurring, image cropping, and another geometrical image processing. On the other hand, there is an unintentionally image modifications such different noises that affect transmitted image like Gaussian noise, and salt & pepper noise. In this context, an image

Table 5 Performance metrics of verification process for different block sizes

Block Size	Image Quality Metrics					
	MSE		PSNR		C_r	
	Cameraman	Reactor	Cameraman	Reactor	Cameraman	Reactor
4×4	52	121.6	31	27.3	0.993	0.989
8×8	16.63	62.4	36	30.2	0.998	0.994
16×16	8.02	29.1	39.12	33.5	0.999	0.997

Table 6 Extracted image with related quality metrics

Extracted Verified Image (No Manipulation)	Image Quality Metrics		
	MSE	PSNR	Cr
	0.050	61.09	0.9993
	0.776	49.17	0.9992
	0.233	34.40	0.9980
	0.082	59.09	0.9997



a- Embedding Hidden Mark Process

b- Verification Process

Fig. 14 Samples of processed images using DCT based algorithm (**a**) Embedding hidden mark, (**b**) Verification process (Cameraman)

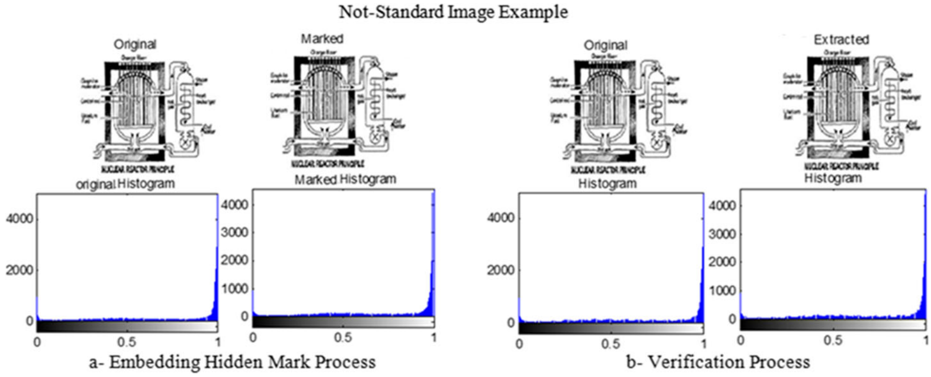


Fig. 15 Samples of processed images using DCT based algorithm (**a**) Embedding hidden mark process, (**b**) Verification process (Reactor/not standard)

resizing, image blurring, Gaussian noise, and salt & pepper noise are selected, provided that a processed large-scale tampering appears visually not detected to accurately evaluate sensitivity of the proposed algorithm. On the other hand, there are unintentional image modifications such as different noises that affect transmitted image like Gaussian noise, and salt & pepper noise. Figure 16 shows the different types of scale-based image manipulation attacks [39, 53].

Figures 17 and 18 show the comparison between the received noisy image and the obtained verified image in the case of Gaussian white noise of mean (0) and variance value (0.00001). In addition, these images are examined in the case of salt-and-pepper noise with rate (0.00005) and are presented in Figs. 19 and 20 respectively. In relation to these two noise types, the results indicate that the proposed model is sensitive to even any small modifications in the image. While the received noisy image and the extracted image appear to be visibly the same. The extracted image (the output of the proposed model) demonstrates a major change compared to the manipulated marked image.

Also, image resizing modification is examined, which a marked image of size (256 × 256) is converted to an image with size (300 × 300) that appears visually unchanged. The received resized image and the output image of the verification process are shown in Figs. 21 and 22, respectively.

The algorithm is proved to have a high sensitivity to detect this type of image manipulation attacks, although the received manipulated image appears to be visually unchanged. The image blurring attack is one of the common sensitive image attacks, which intentionally change the clarity of a whole or sub-image detail. This results in difficult visual extraction of valuable information hidden in blurred areas of a sensitive image that affects the dependable future operations and decisions. It is usually tampering images related to nuclear and medical applications which fine

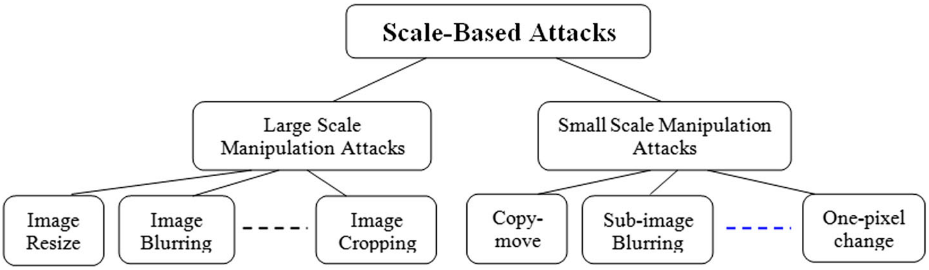


Fig. 16 Categories of scale-based image manipulations attacks

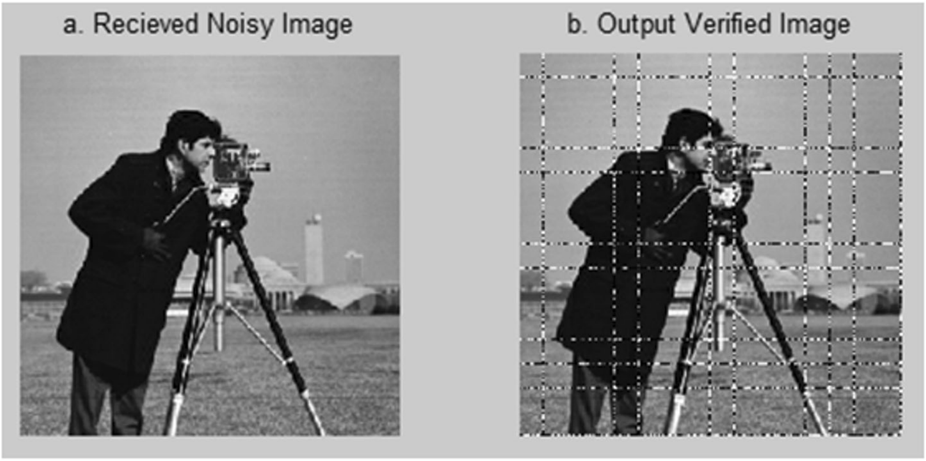


Fig. 17 (**a**) Received noisy image, and (**b**) Output verified image (Gaussian noise (Mean 0 and Variance 0.00001)) for Cameraman image

details of sensitive image are intentionally hidden and the image receiver cannot visually detect a blurred effect. Here, the marked image is blurred using a circular averaging filter with radius 2 to make a tampering act undetectable. Blurred marked image, extracted verified image are compared in case of blurring attack and shown in Figs. 23 and 24, respectively. The results also reveal the high sensitivity of the proposed approach to detect this type of image tampering, although the received tampered image appears to be visually not manipulated.

II. Small Scale and Visually Undetectable Image Manipulation Attacks

Small scale imaging manipulation attacks are those manipulations that affect a small relative area of an intended image. In almost cases, these attacks are mainly intended to a temper, act and usually the tampering cannot be visually detected. This work will focus on studying the capability of the proposed algorithm to identify a copy- move forgery, sub-

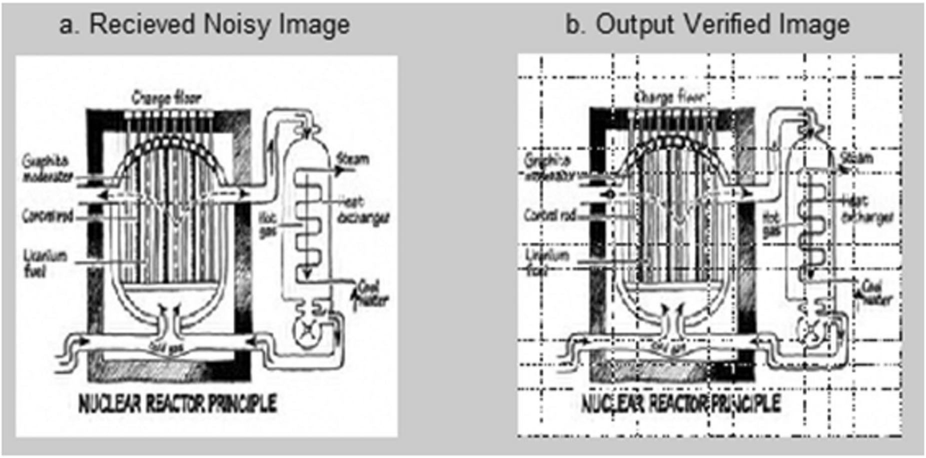


Fig. 18 (**a**) Received noisy image, and (**b**) Output verified image (Gaussian noise (Mean 0 and Variance 0.00001)) for Reactor design image

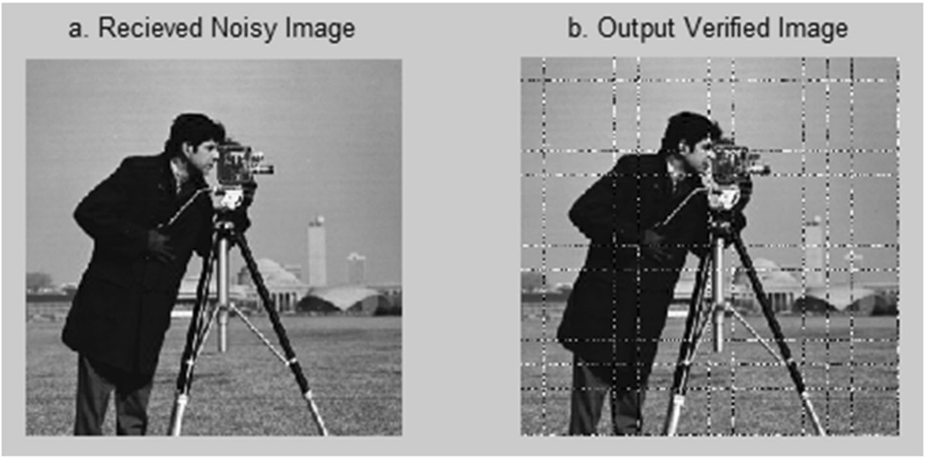


Fig. 19 (**a**) Received noisy image, and (**b**) Output verified image (salt & pepper noise (Rate 0.00005)) for Cameraman image

image blurring attack, and one-pixel change as examples of small-scale image manipulation forgery.

- **Copy-move forgery (Tampered Regions Detection)**

Copy–move forgery is a familiar type of image forgery, in which a dedicated portion of an image is intentionally reproduced and moved to a new part of the same image to change its originality. As an example; replacing included personals faces with others or changing their positions. The proposed algorithm can be also used to detect the tampered areas, which appears clearly in the following results. The marked image is tempered by replacing two small image regions (number of blocks with another number of blocks) which have the same appearance and visible feature. The tampered marked image is intended to appear visibly not

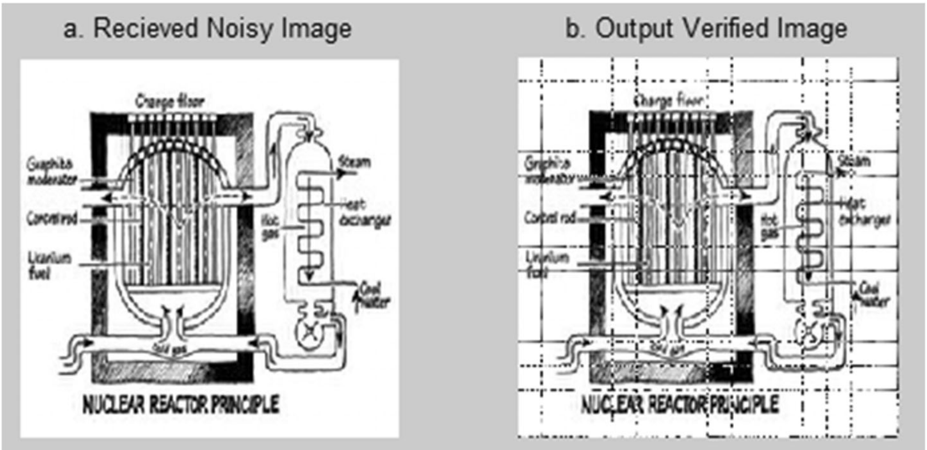


Fig. 20 (**a**) Received noisy image, and (**b**) Output verified image (salt & pepper noise (Rate 0.00005)) for Reactor design image

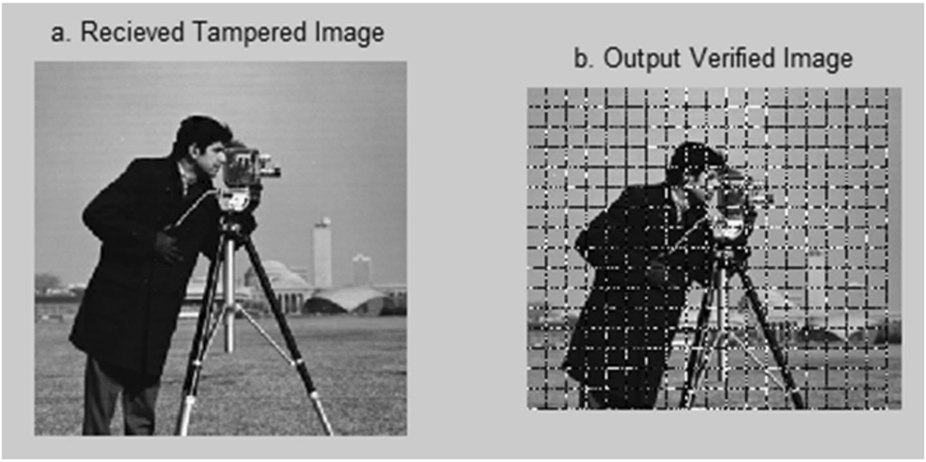


Fig. 21 (**a**) Received tampered image, (**b**) Output verified image in case of image resizing attack (Cameraman)

changed by an attacker as shown in Fig. 25 for reactor design and cameraman images. By processing the tampered image using the verification algorithm, the tampering is detected, in which a forged copy-moving indication appeared visually in the upper half of the extracted image as shown in Fig. 26.

- Sub-image Blurring Attack

A sub-image blurring attack is a type of image manipulations which a small region of the image (small number of blocks) is blurred intentionally to hide an included valuable detail, so the blurred image receiver cannot detect a tampering act. Here a small region of the marked image is blurred using circular averaging filter with radius 10 which the blurring act cannot be detected as shown in Fig. 27. Also; the verification algorithm can detect the tampering in which a forger blurring indication appeared in the upper half of the extracted image as shown in Fig. 28.

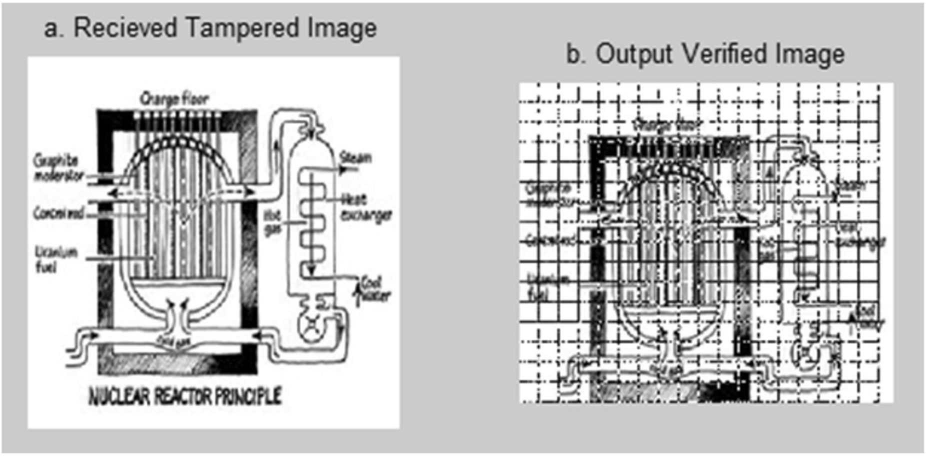


Fig. 22 (**a**) Received tampered image, (**b**) Output verified image in case of image resizing attack (Reactor design)

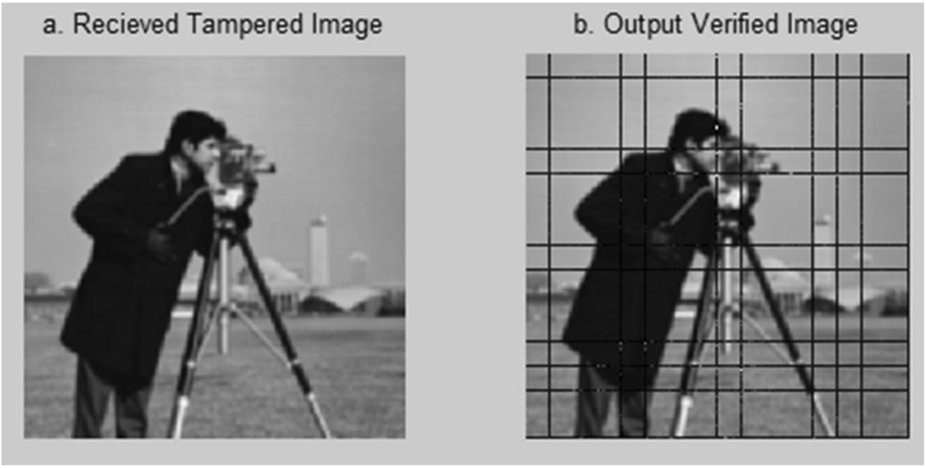


Fig. 23 (**a**) Received tampered image, (**b**) Output verified image in case of image blurring attack (Cameraman)

- **One pixel change manipulation**

This type of image manipulations is discussed to examine the detection sensitivity of the proposed approach when only one-pixel value of marked image is changed intentionally in an imperceptible manner. So, the received manipulated marked image appears to be not tampered as shown in Fig. 29. The output of the verification algorithm in Fig. 30 shows a visual change in the lower half of the extracted image as an indication to one-pixel change manipulation which confirms higher detection sensitivity of the integrity verification algorithm.

In [18], color image steganography is investigated, authors in this paper presented channel dependent payload partition strategy steganography based on amplifying channel modification probabilities. For improving the empirical steganographic security against the channel co-

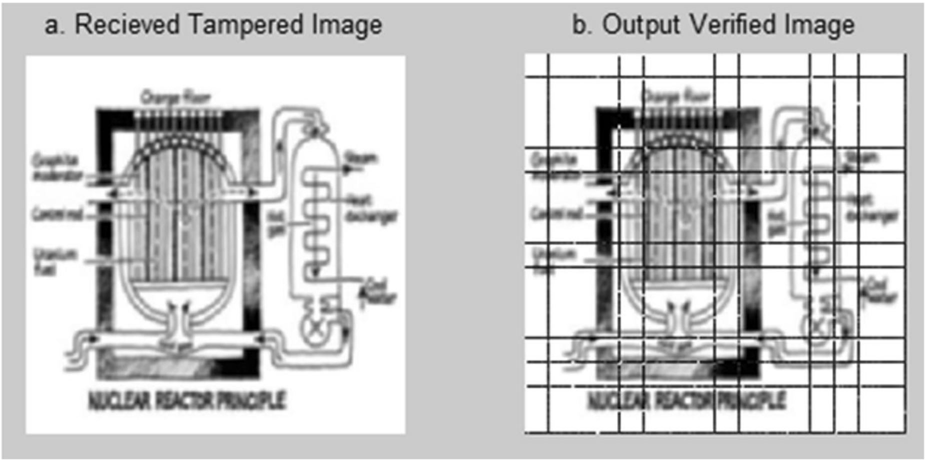


Fig. 24 (**a**) Received tampered image, (**b**) Output verified image in case of image blurring attack (Reactor design)

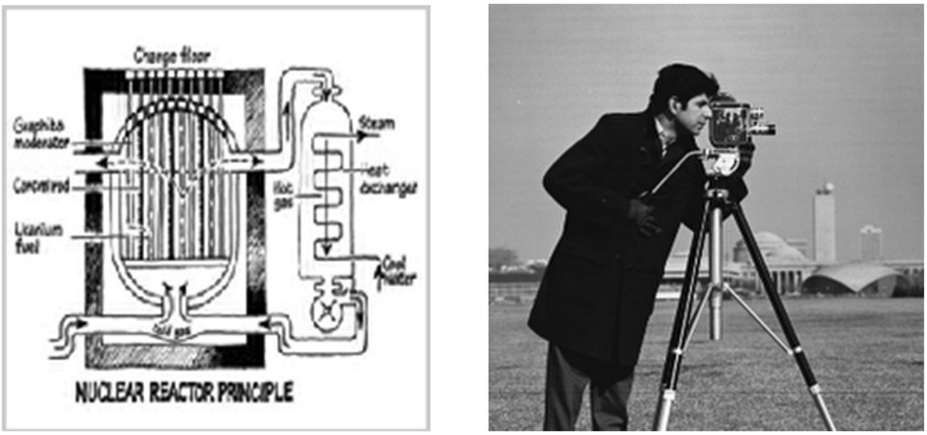


Fig. 25 Tampered images (Copy-move attack)

occurrences detection, the embedding capacity among RGB channels the embedding impacts could be clustered. The experiments of the proposed steganography performance evaluation revealed that its robust and against the modern steganalysis of color images [36].

Data hiding research field importance and its role in the emerging technologies have been discussed in [32]. Authors in [32] presented efficient steganography techniques based on Image Texture Features utilizing adaptive payload distribution in multiple image steganography. Performance of the proposed multiple images steganography has compared to the ordinary single image steganography technique against the modern single image steganalysis, as cleared form the experiments in [31, 38], the payload distribution based steganography performs better against security threats. An efficient Forensic detection technique based on CNN has been proposed in [30].

In the future research plan, the integrity medical data wireless transmission [15] will be considered for enhancing the security Wireless Body Area Networks (WBANs). Also, the

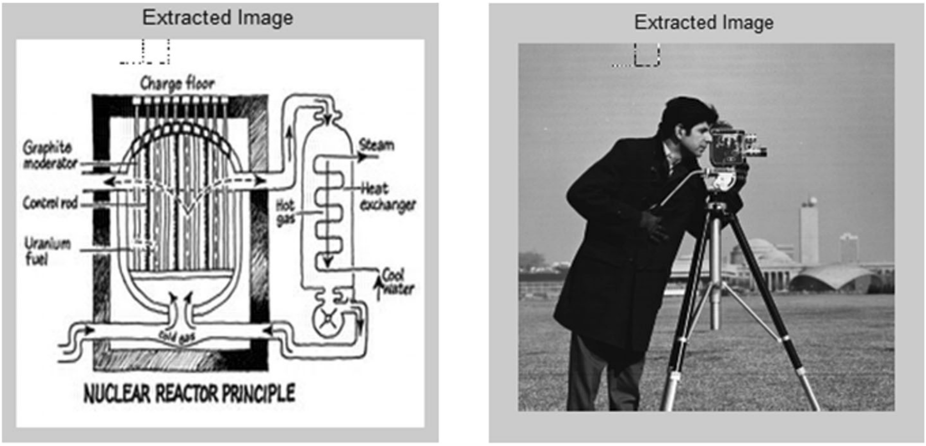


Fig. 26 Extracted verified image

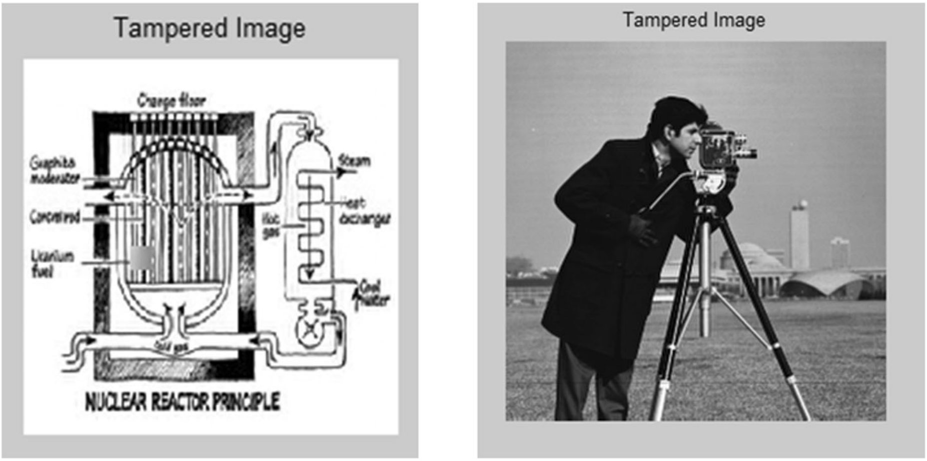


Fig. 27 Tampered images (Sub-image blurring)

encrypted image verification will be presented for double the security of the sensitive images and any secret/authentic documents. The open environment applications require highly secured link for providing reliable transmission media, the encrypted/marked images transmission over the noisy medium will be studied and analyzed with considering the error control schemes utilizing. Also, in the future plan, the complexity of the presented approach will be analyzed with applying another efficient transform technique for decreasing the complexity.

5 Conclusion

Hidden marked algorithm has been presented in this paper to achieve image integrity verification. This DCT based algorithm detects any tiny tampering or forgery in the secret/authentic images. DCT proved to be the most applicable transform to be exploited according to

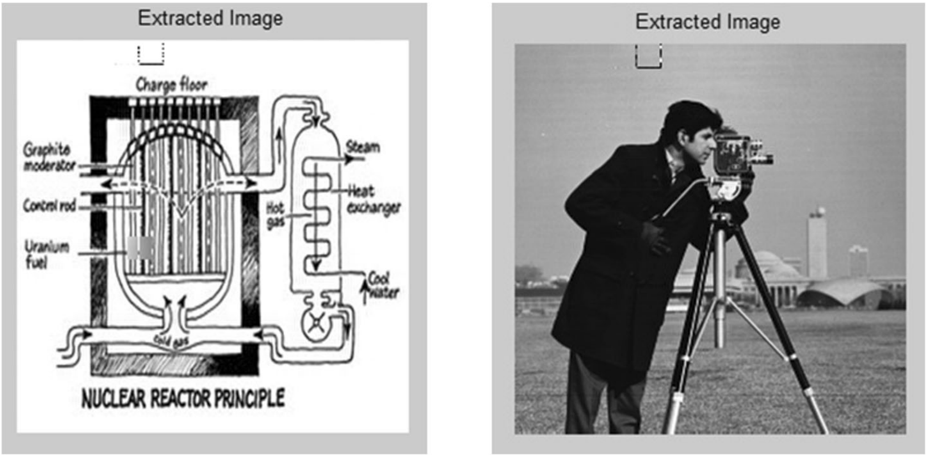


Fig. 28 Extracted verified image

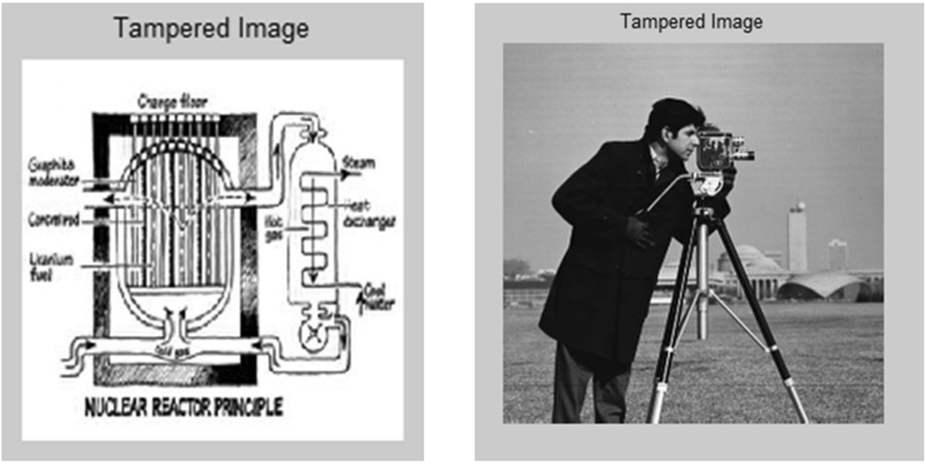


Fig. 29 Tampered images (One pixel change)

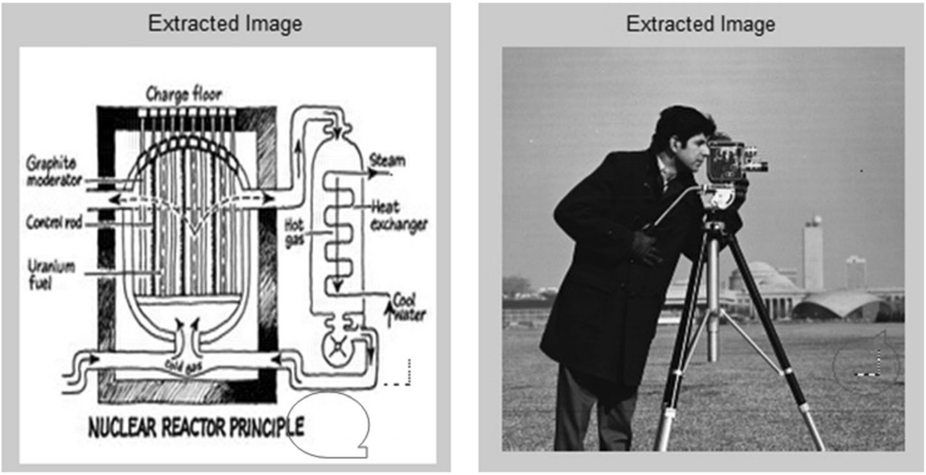


Fig. 30 Extracted verified image

imperceptibility and performance analysis. Both visual and statistical analysis results revealed the higher sensitivity of the approach to detect any image manipulation even they were visually undetectable. So, it can be utilized as an efficient image forgery detection tool for a high confidential data such as nuclear and military applications. In the future work, we are motivated to incorporate the application of a self-multi-level secure scheme with the use of different encryption, steganography and watermarking techniques for vigorous and dependable image communication. Also, the future research plan will include the deep learning-based security techniques for image transmission.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB).

Data availability Author Confirms the data availability which is related to this manuscript in case the requirements for research targets.

Declarations

Conflict of interest Authors declare wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

References

1. Abouelfadl AA, El-Bendary MAM, Shawki F Enhancing transmission over wireless image sensor networks based on ZigBee network. Life Sci J 11(8):342–354
2. Alshanbari HS (2020) Medical image watermarking for ownership & tamper detection. Multimedia Tools Appl
3. Ariatmanto D, Ernawan F (2020) An improved robust image watermarking by using different embedding strengths. Multimedia Tools Appl 79:12041–12067
4. Atawneh S, Almomani A, Al Bazar H, Sumari P, Gupta B (2017) Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. Multimed Tools Appl 76(18): 18451–18472
5. Benrhouma O, Hermassi H, Belghith S (2015) Tamper detection and self-recovery scheme by DWT watermarking. Nonlinear Dynamics 79(3):1817–1833
6. Bhalerao S, Ansari IA, Kumar A (2021) A secure image watermarking for tamper detection and localization. J Ambient Intell Human Comput 12:1057–1068. https://doi.org/10.1007/s12652-020-02135-3
7. Bianchi T, Piva A (2013) Secure watermarking for multimedia content protection: a review of its benefits and open issues. IEEE Signal Process Mag 30(2):87–96
8. Botta M, Cavagnino D, Pomponiu V (2014) Protecting the content integrity of digital imagery with fidelity preservation: an improved version. ACM transactions on multimedia computing. Commun Appl (TOMM) 10(3):29
9. Bouslimi D, Coatrieux G, Roux C (2012) A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images. Comput Methods Prog Biomed 106(1): 47–54
10. Dorgham O, Al-Rahamneh B, Al-Hadidi M, Khatatneh KF, Almomani A (2018) Enhancing the security of exchanging and storing DICOM medical images on the cloud. International Journal of Cloud Applications and Computing 8(1):154–172. https://doi.org/10.4018/IJCAC.2018010108
11. El-Bendary MAM (2017) FEC merged with double security approach based on encrypted image steganography for different purpose in the presence of of noise and different attacks. Multimedia Tools Appl 76(24): 26463–26501
12. El-Bendary MAM, Abou El-Azm AE (2019) Complexity considerations: efficient image transmission over mobile communications channels. Multimed Tools Appl 78:16633–16664. https://doi.org/10.1007/s11042-018-6843-2
13. El-Bendary MAM, Kasban H, Haggag A, El-Tokhy MAR Investigating of nodes and personal authentications utilizing multimodal biometrics for medical application of WBANs security. Multimedia Tools Appl 79(33):24507–24535
14. El-Gohary NM, El-Bendary MAM, Abd El-Samie FE, Fouad MM (2016) Performance evaluation of various erasures coding techniques in digital communication. J Wirel Netw Commun 6(1):10–20

15. Geng L, Zhang W, Chen H, Fang H, Yu N (2020) Real-time attacks on robust watermarking tools in the wild by CNN. J Real-Time Image Process 17:631–641
16. Georgiou T, Liu Y, Chen W, Lew M (2020) A survey of traditional and deep learning-based feature descriptors for high dimensional data in computer vision. Int J Multimedia Info Retrieval 9:135–170
17. Goebel M, Flenner A, Nataraj L, Manjunath BS (2019) Deep learning methods for event verification and image repurposing detection. Electronic Imaging 2019(5):530–1–530-7. https://doi.org/10.2352/ISSN.2470-1173.2019.5.MWSF-530
18. Gupta B, Agrawal DP, Yamaguchi S (2019) Handbook of research on modern cryptographic solutions for computer and cyber security. Noted as an IGI Global Core Reference Title in Security & Forensics. https://doi.org/10.4018/978-1-5225-0105-3
19. Hasan SMK, Ahmad M (2018) Two-step verification of brain tumor segmentation using watershed-matching algorithm. Brain Inf 5:8. https://doi.org/10.1186/s40708-018-0086-x
20. Jararweh Y, Al-Ayyoub M, Fakirah M, Alawneh L, Gupta BB (2019) Improving the performance of the needleman-wunsch algorithm using parallelization and vectorization techniques. Multimed Tools Appl 78(4):3961–3977
21. Kasban H (2016) MAMMK El-Bendary. Performance improvement of digital image transmission over Mobile WiMAX networks. Wirel Pers Commun:1–17
22. Kasban H, Nassar S An efficient approach for forgery detection in digital images using Hilbert–Huang transform", Appl Soft Comput, Vol. No. 97, Part A, Dec. 2020, 106728, https://doi.org/10.1016/j.asoc.2020.106728.
23. Kasban H, Hashima S, Nassar S, Mohamed EM, El-Bendary MAM (2022) Performance enhancing of MIMO-OFDM system utilizing different interleaving techniques with rate-less fountain raptor code.IET Communications. https://doi.org/10.1049/cmu2.12503
24. Kasban H, Nassar S, El-Bendary MAM (2021) Medical images transmission over Wireless Multimedia Sensor Networks with high data rate. Analog Integr Circ Sig Process 108:125–140. https://doi.org/10.1007/s10470-021-01854-7
25. Kaur R, Singh S, Kumar H (2020) TB-CoAuth: text based continuous authentication for detecting compromised accounts in social networks. Appl Soft Comput 97(Part A):106770
26. Kazemi MF, Pourmina MA, Mazinan AH (2020) Analysis of watermarking framework for color image through a neural network-based approach. Complex Intell Syst 6:213–220
27. Korus P (2017) Digital image integrity–a survey of protection and verification techniques. Digital Signal Process 71:1–26
28. Kumar A Design of Secure Image Fusion Technique Using Cloud for privacy-preserving and copyright protection. Int J Cloud Appl Comput (IJCAC) 9(3). https://doi.org/10.4018/IJCAC.2019070102
29. Laouamer L, Tayan O (2015) A semi-blind robust DCT watermarking approach for sensitive text images. Arab J Sci Eng 40(4):1097–1109
30. Liao X, Li K, Zhu X, Liu KJR (2020) Robust detection of image operator chain with two-stream convolutional neural network. IEEE J Selected Topics Signal Processing 14(5):955
31. Liao X, Yin J, Chen M, Qin Z (2022) Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features. IEEE Trans Dependable Secure Comput 19(2):897–911. https://doi.org/10.1109/TDSC.2020.3004708
32. Liao X, Yu Y, Li B, Li Z, Qin Z A new payload partition strategy in color image steganography. IEEE Trans Circ Syst Video Technol 30(3)
33. Liu J-e, An F-P Image classification algorithm based on deep learning-kernel function. Sci Program J 2020: 7607612. https://doi.org/10.1155/2020/7607612
34. Mamta BBG An efficient KP design framework of attribute-based searchable encryption for user level revocation in cloud. Special issue paper, wileyonlinelibrary.com/journal/cpe. https://doi.org/10.1002/cpe.5291
35. Mohamed El-Bendary MAM, Abou-El-azm AE, El-Fishawy NA, Shawki F, Abd-ElSamie FE, El-Tokhy MAR, Kazemian HB (2012) Performance of the audio signals transmission over wireless networks with the channel interleaving considerations. J Audio Speech Music Proc 2012:4. https://doi.org/10.1186/1687-4722-2012-4
36. Mahmoud MEA, Xuemin (Sherman) S (2014) Security for multi-hop wireless networks. Springer International Publishing. https://doi.org/10.1007/978-3-319-04603-7
37. Mu Y, Zhou Z (2019) Visual vocabulary tree-based partial-duplicate image retrieval for coverless image steganography. Int J High Perform Comput Netw 14(3). https://doi.org/10.1504/IJHPCN.2019.102133
38. Nassar SS, Mohsen AM (2022) El-BendaryConfidentiality considerations: multimedia signals transmission over different wireless channels utilized efficient secured model. Multimed Tools Appl 81:25707–25744. https://doi.org/10.1007/s11042-022-12297-1

39. Nassar SS, Ayad NM, Kelash HM, El-Sayed HS, El-Bendary MAM, El-Samie A, Fathi E, Faragallah OS Content verification of encrypted images transmitted over wireless AWGN channels. Wireless Personal Comm 88(3):479–491
40. Nassar SS, Ayad NM, Kelash HM, El-Sayed HS, El-Bendary MAM, Abd El-Samie FE, Faragallah OS (2016) Efficient audio integrity verification algorithm using discrete cosine transform. Int J Speech Technol 19:1–8. https://doi.org/10.1007/s10772-015-9312-6
41. Nassar SS, Faragallah OS, El-Bendary MAM (2021) Reliable mark-embedded algorithm for verifying archived/encrypted image contents in presence different attacks with FEC utilizing consideration. Wireless Pers Commun 119:37–61. https://doi.org/10.1007/s11277-021-08176-x
42. Parah SA, Sheikh JA, Ahad F, Loan NA, Bhat GM (2017) Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimed Tools Appl 76(8):10599–10633
43. Pourhadi A, Mahdavi-Nasab H (2020) A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain. Multimedia Tools Appl 79:21653–21677
44. Robert L, Shanmugapriya T (2009) A study on digital watermarking techniques. Int J Recent Trends Eng 1(2):223
45. Shih FY (2017) Digital watermarking and steganography: fundamentals and techniques. CRC press. https://doi.org/10.1201/9781315121109
46. Sultana F, Charles S, Govardhan A (2013) A tamper proof noise resilient end to end image based authentication system over wireless transmission with AWGN channel using wavelet based templates and AES. IJCSNS Int J Comput Sci Network Secur 13(5):41–48
47. Tsougenis ED, Papakostas GA, Koulouriotis DE, Tourassis VD (2012) Performance evaluation of moment-based watermarking methods: a review. J Syst Softw 85(8):1864–1884
48. Urvoy M, Goudia D, Autrusseau F (2014) Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. IEEE Trans Info Forensics Sec 9(7):1108–1119
49. Von Solms R, Van Niekerk J (2013) From information security to cyber security. Comput Sec 38:97–102
50. Xu G, Lai M, Li J, Sun L, Shi X (2018) A generic integrity verification algorithm of version files for cloud deduplication data storage. EURASIP J Info Sec
51. Xu H, Ma Y, Liu H-C, Deb, Liu H, Tang J-L, Jain AK (2020) Adversarial attacks and defenses in images, graphs and text: a review. Int J Autom Comput 17:151–178
52. Yang L, Song Q, Wu Y (2020) Attacks on state-of-the-art face recognition using attentional adversarial attack generative network. Multimed Tools Appl 5(Sept.):855–875
53. Yu C, Li J, Li X, Ren X, Gupta BB (2018) Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimedia Tools Appl 77:4585–4608

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