utilizing random forest, refrigeration, and the violet conversion method to improve the medical digital picture encryption algorithm

Mustafa Abdulkadhim Mejbel [1,2]
[1]Department of Computer Engineering, Software, Azad University, Khorsakan Branch, Isfahan
[2]College of Computer Science, Al-Rafidain University College, Baghdad

Abstract

Digital photos may now be copied, edited, and distributed more easily, quickly, and without sacrificing quality thanks to the Internet. Data security and privacy are at risk when network technology advances quickly. Consequently, in order to meet the difficulties and hazards associated with the preservation of digital information, content authentication, copyright protection, and duplicate prevention are crucial. Illegal copying and distribution of digital content using physical transmission media is a simple process. Any digital content such as images, audio and video can hide data. Digital image watermarking provides an alternative solution to ensure tamper resistance, intellectual property and enhance the security of multimedia documents. Digital image watermarking is a technique in which watermark data is embedded in a multimedia product and later extracted from or identified in the watermarked product. In this research, a digital image watermarking method is introduced with the help of random forest algorithm and refrigeration algorithm in the field of violet transformation. In this method, the important output parameters of the hidden mining algorithm are improved with the help of the Violet transformation, because in recent years, the ease of producing, manipulating and falsifying digital data has led to providing new, innovative and more useful methods for securing digital data. According to the results, by comparing the PSNR of two hidden images and the base image, it can be seen that the proposed method has a very good score, so that the PSNR of the proposed method is 197.7. On the other hand, in order to check the proposed algorithm in the effect of various attacks, simulations were carried out in the form of 4 attacks of cutting the image, adding noise, changing the contrast, and finally applying the JPEG compression algorithm to the image. The first attack that was mentioned was the image cropping attack. If this attack takes place exactly in the place that was chosen to insert the information, the information will be lost, but if it happens in another place, it will not lead to the deletion of the information. The results show the good resistance of this method in maintaining the inserted information.

Keywords: Violet transform algorithm, medical digital images, reversible cryptography, radiology image, improvement of cryptography algorithm

المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية
Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN 2790-1254
العدد13 حزيران 2024
No.13 June 2024

استخدام الغابة العشوائية والتبريد وطريقة التحويل البنفسجي لتحسين خوارزمية تشفير الصور الرقمية الطبية

مصطفى عبدالكاظم مجبل [1,2]
[1]ماجستير / هندسة الحاسبات /البرمجيات / جامعة ازاد الاسلامية /اصفهان فرع خورسكان /ايران
[2]بكالوريوس/علوم الحاسبات / كلية االرافدين الجامعة /بغداد/العراق
Corresponding author's email: iraq.it2012@gmail.com

خلاصة

يمكن الآن نسخ الصور الرقمية وتحريرها وتوزيعها بسهولة أكبر وبسرعة ودون التضحية بالجودة بفضل الإنترنت. يتعرض أمان البيانات والخصوصية للخطر عندما تتقدم تكنولوجيا الشبكات بسرعة. وبالتالي، ومن أجل مواجهة الصعوبات والمخاطر المرتبطة بالحفاظ على المعلومات الرقمية، فإن مصادقة المحتوى، وحماية حقوق النشر، ومنع التكرارات أمر بالغ الأهمية. يعد النسخ والتوزيع غير القانوني للمحتوى الرقمي باستخدام وسائط النقل المادية عملية بسيطة. يمكن لأي محتوى رقمي مثل الصور والصوت والفيديو إخفاء البيانات. توفر العلامة المائية للصور الرقمية حلاً بديلاً لضمان مقاومة العبث والملكية الفكرية وتعزيز أمان مستندات الوسائط المتعددة. العلامة المائية للصور الرقمية هي تقنية يتم فيها تضمين بيانات العلامة المائية في منتج متعدد الوسائط ثم يتم استخراجها لاحقًا من المنتج الذي يحمل علامة مائية أو تحديدها فيه. في هذا البحث تم تقديم طريقة العلامة المائية للصورة الرقمية بمساعدة خوارزمية الغابة العشوائية وخوارزمية التبريد في مجال التحول البنفسجي. في هذه الطريقة، يتم تحسين معلمات الإخراج المهمة لخوارزمية التعدين المخفية بمساعدة التحويل البنفسجي، لأنه في السنوات الأخيرة، أدت سهولة إنتاج البيانات الرقمية ومعالجتها وتزويرها إلى توفير طرق جديدة ومبتكرة وأكثر فائدة للتعدين. تأمين البيانات الرقمية. وفقا للنتائج، من خلال مقارنة PSNR لصورتين مخفيتين والصورة الأساسية، يمكن ملاحظة أن الطريقة المقترحة حصلت على درجة جيدة جدا، بحيث يكون PSNR للطريقة المقترحة 197.7. من ناحية أخرى، ومن أجل التحقق من تأثير الخوارزمية المقترحة على الهجمات المختلفة، تم إجراء عمليات المحاكاة على شكل 4 هجمات تتمثل في قطع الصورة، وإضافة الضوضاء، وتغيير التباين، وأخيراً تطبيق خوارزمية الضغط JPEG على الصورة. صورة. الهجوم الأول الذي تم ذكره كان هجوم اقتصاص الصورة. إذا حدث هذا الهجوم بالضبط في المكان الذي تم اختياره لإدراج المعلومات، فسيتم فقدان المعلومات، أما إذا حدث في مكان آخر فلن يؤدي إلى حذف المعلومات. وأظهرت النتائج المقاومة الجيدة لهذه الطريقة في الحفاظ على المعلومات المدخلة.

الكلمات المفتاحية: خوارزمية التحويل البنفسجي، الصور الرقمية الطبية، التشفير العكسي، الصورة الشعاعية، تحسين خوارزمية التشفير

1 Introduction

Given how simple it is to modify any image, digital image authentication is a crucial concern for the digital revolution. Verifying the legitimacy of digital photos has become a top priority for researchers in recent years. To address this issue, a number of appropriate watermarking techniques have been developed based on the intended applications. Attaining a watermarking system that is both reliable and safe is challenging, though. The standard requirements utilized in the creation of watermarking techniques for multiple distinct applications are listed in this research along with specifics about standard watermarking system frameworks. The most recent developments in digital picture watermarking strategies are also examined to

identify cutting-edge approaches and their drawbacks. Future research directions are suggested, and a few frequent assaults are highlighted. Digital media has several distinct advantages over analog media, such as high quality, easy editing, high performance, and simple reproduction. High diffusion of broadband networks and new developments in digital technology have made ownership protection and authentication of digital multimedia a very important issue. Picture handling and the Web have made it more straightforward to repeat, change, replicate, and disseminate advanced pictures for minimal price and with close moment conveyance without loss of value. Network innovation is quickly creating and improving, which undermines information protection and security. In this way, satisfied validation, copyright assurance and duplication security assume a fundamental part in confronting the difficulties of existing and future dangers in saving advanced data. Advanced picture watermarking is essentially the computerized watermarking of a picture that gives an elective answer for guarantee alter opposition, protected innovation proprietorship, and improved security of interactive media reports. Any computerized content, for example, pictures, sound and video can conceal information. Computerized content can without much of a stretch be illicitly moved by, and disseminated through an actual transmission medium during correspondence, data handling, and information stockpiling. Computerized picture watermarking is a method wherein watermark information is implanted in a media item and later separated from or recognized in the watermarked item. These strategies guarantee alter opposition, confirmation, content check and picture respectability [1]. It is exceptionally difficult to eliminate the watermark by showing or changing over the watermarked information to other record designs. Thusly, after an assault, change data can be acquired from the watermark. It is vital to recognize computerized watermarking and different innovations, for example, encryption [2]. Computerized to-simple transformation, pressure, document design change, re-encoding, and disentangling can likewise endure advanced picture watermarking methods. These capabilities supplant (or supplement) cryptography. The data is implanted in the substance and can't be taken out by ordinary use [3].

The word Steganography is gotten from the Greek word Steganos. This procedure conceals the correspondence and changes the picture so just the expected shipper and recipient can distinguish the message being sent. This procedure makes discovery more troublesome. Rather than encoding messages, steganography can be utilized to conceal them in other non-hostile articles, so their reality isn't found and, in this manner, can be utilized as an elective method for protection and security. In any case, because of the quick development of the Web and PC organizations, steganography can be utilized as an instrument to trade data and plan psychological oppressor assaults [3]. Steganography conceals the presence of an overlay picture,

while watermarking strategy implants a message in the genuine substance of the computerized signal in the actual sign. Hence, a snoop can't erase or supplant a message to get an active message. To safeguard the substance from unapproved access, implanting the data in the principal image is important. Advanced picture watermarking is intangible and hard to eliminate by unapproved people. This method has been carried out by different calculations utilizing spatial and recurrence spaces, each of which has its own distinct advantages and limitations.

This chapter includes the statement of the problem, the necessity of conducting the research, the goals and hypotheses of the research, the definition of the variables and assumptions of the research and the definition of the terms, which will be explained in detail in the following. The importance of the present research problem is that digital information hiding methods are widely used to maintain the security of digital data. One of the most widely used types of digital data are digital images. In order to maintain the security of digital images, information is secretly embedded in them as secret information (watermark).

1.1 The Statement's Issue

These days, digital content may be distributed over communication channels with ease because of the Internet's, multimedia systems, and worldwide computer networks' explosive expansion. Digital image watermarking, taking into consideration that it is a research field, provides a platform for researchers and attempts to shield advanced data from unlawful obtaining, propagation, control, use, and dissemination through actual transmission media during correspondence, data handling, and information stockpiling. Research watermarking started as soon as 1982, and in this way, advanced watermarking methods have improved by coordinating settings, quality, and examination amount contemplations. Watermarks have been broadly used to improve security [4]. Advanced watermarking PC innovation showed up in 1988, giving classification, honesty, and accessibility, and starting around 1995, different developments connected with computerized picture watermarking have been consolidated. In watermarking strategies, an image of the proprietor's genuineness (watermark) is implanted in the host sign, and this watermark information can be removed later. Watermark information, which might be noticeable or undetectable, can comprise of a solitary piece, a bunch of paired information, or various examples in the host signal [5].

To emulate the human visual discernment framework, data entropy assumes a fundamental part in advanced picture watermarking plan. To accomplish the ideal harmony between intangibility, strength, and limit of a computerized picture watermarking innovation, data entropy can be taken advantage of through a recognizable just (JND) model [6]. Data entropy can be characterized with regards

to the encompassing impact and can be utilized to decide the situations where information is embedded. This situation limits perceptual mutilation and gives better heartiness and great physicality.

To safely convey a message, the cycle starts with a cover picture (have picture). The host picture can be dealt with just as commotion, clamor with superfluous data, or as a media message to be communicated. Watermarked information goes over a correspondence channel that might be lossy, uproarious, or untrustworthy. Subsequently, watermarked information might experience the ill effects of potential assaults, including lossy pressure, mathematical bending, signal handling tasks, and sign change, and so forth. That is, there might be a distinction between the first watermarked information and the got information [8]. A watermarked picture goes through a correspondence channel that produces commotion. This clamor expands the data entropy [9], which builds the vulnerability or vagueness of the typical data in a picture. Hence, watermarking methods must be applied to high-goal pictures and complex examples that have higher data entropy. Subsequently, to work on the security, the scrambled picture ought to be handled so that the picture reproduction is hearty. Another optical picture encoding strategy gets the encoded picture with an irregular stage encoding procedure in both information and Fourier planes [10], where two arbitrary stage planes in the information and Fourier planes are supplanted by two deformable mirrors. Separately. Thusly, the framework can accomplish the ideal pillar shape in the plentifulness and stage data of the picture [11].

Information encryption is the act of hiding information in multimedia data (image, audio or video) for various applications such as proving ownership rights, checking the authenticity of image content and non-falsification of an image, and controlling the number of printed copies of a work. Information encryption methods are used when information and a message need to be secretly embedded in a medium such as image, sound, video, etc. In image encryption, the embedding of information in the images should be such that small changes are applied to the original image and the encrypted image is not significantly different from the original image in terms of the human vision system [3].

In this research, we will introduce a digital image watermarking method with the help of random forest algorithm and refrigeration algorithm in the field of violet transformation. With this aim, in which we will improve the important output parameters of the hidden mining algorithm with the help of Violet transformation, because in recent years, the ease of producing, manipulating and falsifying digital data has led to providing new, innovative and more useful methods for securing digital data. Encrypting or watermarking information in digital images is a way to

ensure the security of digital images. While the traditional information encryption methods were irreversible. This means that after hiding the information in the content and sending the encrypted version to the recipient, it was not possible to recover the original image and perform evaluations on the original version. This feature made traditional information encryption methods unusable in sensitive cases that require the original content without the slightest change. For this reason, new encryption methods called reversible methods were used. The distinctive feature of reversible encryption methods is that on the receiver side, after extracting the encrypted watermark, there is the ability to recover the original content before encryption.

1.2 The significance and requirement of carrying out research

In order to preserve digital information in the face of current and potential threats, content authentication, copyright protection, and duplication prevention are crucial. The process of digitally watermarking an image to assure tamper resistance, intellectual property ownership, and improved security of multimedia documents is known as computerized picture watermarking. Computerized media, including sound, video, and illustrations, can all disguise information. With regards to correspondence, data handling, and information stockpiling, computerized content can be promptly gotten, recreated, and sent illicitly by means of an actual transmission media. Computerized picture watermarking is a procedure where watermark information is implanted in a sight and sound item and later separated from or recognized in the watermarked item. These strategies guarantee alter obstruction, validation, content confirmation and picture respectability [1]. It is exceptionally difficult to eliminate the watermark by showing or changing over the watermarked information to other document designs. Thusly, after an assault, change data can be acquired from the watermark. It is critical to recognize computerized watermarking and different innovations, for example, encryption [2]. Advanced to-simple transformation, pressure, document design change, re-encoding, and deciphering can likewise endure computerized picture watermarking procedures. These capabilities supplant (or supplement) cryptography. The data is implanted in the substance and can't be taken out by ordinary use [3].

1.3 The element of novelty and creativity in research

This study reviews the broad backdrop and the framework of general watermarking methods, which are divided into watermark embedding and extraction operations. The following subsections include a set of standard design standards for assessing the effectiveness of watermarking systems. Watermarking systems are described as a highly specialized research topic with related applications. A review of digital picture watermarking methods is given below, based on the scope of work. The study findings from the advanced techniques that were covered are then summarized, and

the latest developments in this subject are explained using a table that serves as a transmission medium for data during processing, communication, and storage. Then, we show a few regular assaults or dangers that ought to be considered as a test to plan an effective framework. Execution measurements, for example, top sign to-commotion proportion (PSNR), underlying similitude file (SSIM), mean squared blunder (MSE), and standardized cross-relationship (NCC), are likewise momentarily portrayed. In the previous works and in the base article, analytical work has been done on the basis of neural network, but in this research, we are trying to implement the implementation work in MATLAB software by using Hub algorithm, so as to solve the shortcomings that were mentioned in the second and third chapters of the research. are reviewed to be largely resolved.

1.4 The particular goals of the study

1. Image detection and normalization
2. Protecting digital photos from harm using the suggested encryption techniques
3. Digital image resistance encryption using the random forest and refrigeration algorithms

1.5 Research inquiries

1. What are the drawbacks of the watermarking methods now in use?
2. Which picture watermarking strategies are popular right now?
3. What specifications apply to image watermarking methods?
4. How precisely does the discrete wave transformation algorithm work during retrofitting, and how can its efficiency be increased?

1.6 Research hypotheses

• The properties of digital images allow for the whole removal of flaws by masking techniques based on the discrete wavelet algorithm and cooling. Refrigeration algorithm, along with the hub algorithm, creates a point-by-point detection feature for the desired system, and by using them, the entire image can be covered and checked.

2 The studied variables

After getting the general form of the proposed method and algorithm, in this case, enter the code for the desired system into MATLAB and according to the variables written as assumptions in the work, this system in the MATLAB calculation program and according to The process we consider for the desired system will be the process of analyzing the results. Execution measurements, for example, top sign to-clamor proportion (PSNR), underlying comparability list (SSIM), mean squared blunder

(MSE), and standardized cross-relationship (NCC), are additionally momentarily portrayed. The information related to the type of variable, definitions and how to measure them are described in table (1-1).

Table 1 Research variables

scale	How to measure the variable	Variable scientific-practical definition	Variable type: a little discrete	Variable type: a little continuous	Variable type: Dependent	Variable type: Independent	Variable type: Background	variable title	row
Number	Image specifications	The number of pixels in an image	✓			✓		The number of pixels	1
Number	Image specifications	Image dimensions in pixels	✓			✓		Image dimensions	2
Percent	$PSNR = 20 * log(max(max(f)))/((MSE)\text{^}0.5)$	Peak signal to noise ratio	✓		✓			*PSNR*	3
Percent	$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$	Structural similarity index	✓		✓			*SSIM*	4
Percent	$MSE = (1/(m * n)) * sum(sum((f - g).\text{^}2))$		✓		✓			*MSE*	5

3 Literature and research background

History of reversible encryption of information in images

3.1 Types of information encryption methods in terms of fragility

Right now, because of the quick development of worldwide PC organizations, the Web, and media frameworks, computerized content can be handily appropriated through correspondence channels. To shield computerized data from unlawful procurement, proliferation, control, use and circulation through actual transmission media during correspondence, data handling and information stockpiling, advanced

picture watermarking, taking into account it as an exploration field, gives a stage to It makes specialists.

Research watermarking started as soon as 1982, and hence, advanced watermarking strategies have improved by coordinating examination settings, quality, and amount contemplations. Watermarks have been broadly used to improve security [4]. Advanced watermarking PC innovation showed up in 1988, giving classification, honesty, and accessibility, and starting around 1995, different developments connected with computerized picture watermarking have been consolidated. In watermarking strategies, an image of the proprietor's legitimacy (watermark) is implanted in the host sign, and this watermark information can be separated later. Watermark information, which might be noticeable or undetectable, can comprise of a solitary piece, a bunch of parallel information, or various examples in the host signal [5].

To mirror the human visual discernment framework, data entropy assumes a fundamental part in the advanced picture watermarking plan. To accomplish the ideal harmony between impalpability, vigor, and limit of a computerized picture watermarking innovation, data entropy can be taken advantage of through an observable just (JND) model [6]. Data entropy can be characterized regarding the wrapping impact and can be utilized to decide the situations wherein information is embedded. This situation limits perceptual contortion and gives better power and great physicality. Information encryption methods can be classified into three categories: fragile, semi-fragile and resistant.

4 Research literature

In this section, a number of methods presented in the field of reversible encryption are described. One of the methods [15] chooses the best region of the cover picture to embed the watermark to accomplish better intangibility. In some cases, a noticeable watermark in a picture is favored [16]. Be that as it may, imperceptible checking frameworks are more famous. Imperceptibility might be utilized in advanced imaging, telemedicine, computerized documentation, and so on.

4.1 The first method - Fragile reversible cryptography by improving the multilayer embedding method

In 2013, a reversible cryptographic method based on the improvement of the difference propagation multilayer embedding method was presented [6]. There are a few general ways to deal with accomplish high heartiness, like repetitive installing, wide range, and watermark implanting, and so forth. Subsequently, a decent computerized picture watermarking framework ought to be hearty against different assaults, with the goal that unapproved wholesalers can't eliminate or erase the watermarked information. Contingent upon the application, not all watermarking

calculations might have a similar degree of strength. Some are vigorous against different picture handling activities, while others come up short against different assaults [17]. In the methods of expanding the embedding difference in the edges and non-uniform areas, it causes a serious drop in the quality of the image. For a pair of gray level values, after performing the embedding with the difference expansion method, the new gray level values are obtained, since the mean value remains unchanged, so relations (1-2) and (2-2) hold:

$$x - x' \approx y - y' \tag{2-1}$$

$$\begin{aligned}(x-x')^2 + (y-y')^2 &\approx 2.(y-y')^2 \\ &= 2.\left(\left\lfloor \frac{h}{2} \right\rfloor - \left\lfloor \frac{h'}{2} \right\rfloor\right)^2 \approx \frac{h^2}{2}\end{aligned} \tag{2-2}$$

Therefore, the Euclidean distance between and is proportional to the difference value h. To minimize the mean squared error between the original image and the embedded image, the difference values should be chosen with a small value to expand the difference. An algorithm based on full-stage bi-symmetrical change (APBT) and solitary worth deterioration (SVD) [22] is proposed to accomplish better strength and impalpability of the watermarking framework, where the block-based APBT calculation is applied to a particular area. Is. Acquired from the property scores of the chose competitor. APBT coefficients produce the coefficient framework for SVD to install the watermark. Moreover, a discrete wavelet changes (DWT), all-stage discrete cosine dipole changes (APDCBT) and SVD-based strategy to build the subtlety and vigor, in which high-recurrence direct current (DC) coefficients are proposed. The sub groups (LH) and (HL) are utilized to install the watermark picture. This strategy has been demonstrated to be vigorous against many sign handling activity. First, the average of the three-color components for each pixel is determined and then stored in the matrix A The relation (2-3) is used to generate the watermark

$$x_{n+1} = f\left(x_n\right) = 4\sin^2\left(x_n - 2.5\right) \tag{2-3}$$

For each value belonging to A, an initial value is calculated based on the equation (2-4).

$$seq\left(k,0\right) = a.\left\lfloor \frac{s(k)}{2^l} \right\rfloor .2^l + b.pos + c.key \tag{2-4}$$

In relation (2-4), seq(k,0) determines the initial value for the kth pixel. s(k) determines the value corresponding to the kth pixel of A. c,b,a and l are

predetermined constants pos determines the location index of the kth pixel and key is the key used for the security of the encryption method. For the size image, the value of pos for the pixel located at the coordinate (i,j) is equal to M.i+j, after the value of seq(k,0) is determined for the kth pixel, this value is used as input given to equation (2-3), the resulting output will be seq(k,1). Again, the value of seq(k,1) is given as an input to the equation (2-3) and the resulting output will be seq(k,2), this procedure continues until seq(k,I) is obtained (seq(k,i)) i=1,2,3,...,I) in this way, for the kth pixel there will be a sequence of length I. Now this relation is converted into a binary string of length I based on relation (2-5).

$$b\_seq(k,i)=\begin{cases}1 & if \quad seq(k,i)>T\\ 0 & if \quad seq(k,i)\le T\end{cases} \qquad (2\text{-}5)$$

4.2 The second method - Reversible encryption method using a new sorting criterion

This method is an improvement on the method presented by Sachno et al. [9]. Watermark limit (otherwise called payload) assesses how much data that can be implanted in the host picture, in view of the size of the first information. Limit is characterized by the quantity of pieces that each host picture conveys subsequent to embedding the watermark picture. In any case, implanting watermark data is all the more a troublesome errand that requires essentials in light of reasonable applications [1]. At the end of the day, the limit decides the constraints of watermarking data while fulfilling the power and indistinctness of watermarking. The data accessible to the assailants, the information encoder and decoder, twisting cutoff points, and the factual model utilized in the cover picture decide the watermark limit [27]. There are different strategies to assess the issues of watermarking limit under assaults. These incorporate game hypothetical methodologies and equal Gaussian channels (PGC).

Then again, watermark extraction is effective just when the channel limit is more prominent than the quantity of pieces implanted in the host picture [28]. Watermarking limit is characterized by location likelihood, deception likelihood and mean squared mistake. At the point when more watermark information is embedded into the host picture, more bending is apparent. Be that as it may, mutilation can't go on without serious consequences in military and clinical applications. Accordingly, watermarking procedures ought to be executed to limit mutilation with less information inserting limit. In such manner, a mix of IWT (whole number wavelet change), bitmap strategy and a QR (speedy reaction) code has been proposed [29], where the watermark is changed over into a QR code. In this manner, the proposed strategy decreases the implanting limit.

Here is an example to solve this problem. Suppose there are two cells named a and b, as shown in figure (1-2), a is a rough cell and b is a smooth cell.

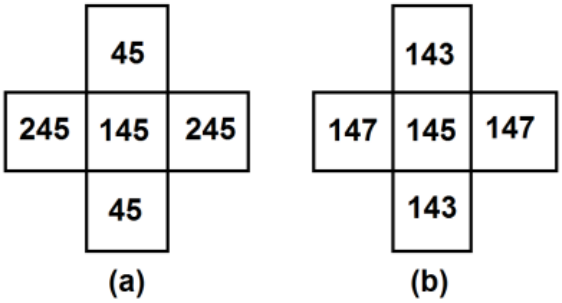


Fig 1 shows smooth cell b and rough cell a

It is obvious that cell b is more suitable for embedding and it is expected that the value of local variance for cell a is larger than cell b and the sorting process of cell b appears before cell a, but the value of local variance for both of these cells is equal to zero, so using The local variance criterion for missorting introduces these two cells in the co-sorting process. In this method, to solve this problem, a new criterion for more accurate sorting is presented. First, it is calculated by the equation (2-6).

$$\lambda_{i,j} = \frac{p_1 + p_2 + p_3 + p_4}{4} \qquad (2\text{-}6$$

$$p_1 = \left(v_{i-1,j} - v_{i,j+1}\right)^2 , p_2 = \left(v_{i,j+1} - v_{i+1,j}\right)^2$$

$$p_3 = \left(v_{i+1,j} - v_{i,j-1}\right)^2 , p_4 = \left(v_{i,j-1} - v_{i-1,j}\right)^2$$

For the cells displayed in Figure (1-2), the worth of nearby difference for the two cells is zero, yet the incentive for cell an is equivalent to 200 and for cell b is equivalent to 4. By utilizing for arranging, it tends to be perceived that cell b is more reasonable for implanting than cell a. A little worth demonstrates a little expectation mistake and consequently shows a smooth cell. The computational expense for implanting the watermark in the host picture and extricating the watermark from the watermarked picture ought to be negligible. This cost incorporates two central concerns - the complete time expected for watermark implanting and extraction, and the absolute number of embedders and identifiers associated with the watermarking procedure. A decent compromise among power and computational intricacy should be kept up with. It has been executed in reference [30] to guarantee the security and power of tiny pictures. To all the more precisely gauge the intricacy around a pixel,

it is important to utilize a bigger neighborhood district, for instance, a locale rather than a little locale [10]. This region is displayed in figure (2-2).

O	X	O	X	O	X	O
X	O	$u_{i-1,j-1}$	O	$u_{i-1,j+1}$	O	X
O	$u_{i,j-2}$	O	$u_{i,j}$	O	$u_{i,j+2}$	O
X	O	$u_{i+1,j-1}$	O	$u_{i+1,j+1}$	O	X
O	X	O	X	O	X	O

Fig 2 neighborhood area around the pixel [10]

4.3 The third method - Reversible cryptography based on the fuzzy method

This method has improved the reversible image encryption presented by Al-Qureshi and Kho [11] in two parts [12]. The watermark key is the mystery key that decides specific boundaries of the implanting capability. This key contains a subset of picture coefficients, inserting heading as well as installing range. Watermark key assessment and planning is significant on the grounds that it decides the level of safety of the watermark framework and relies upon specific boundaries, for example, the implanted message and the watermark picture [33]. In this way, for the implanting and extraction process, a mystery key is expected to guarantee security. The mystery key comprises of a confidential key, a recognizable proof key and a public key. The confidential key is simply accessible to the client, the confirmation key is checked in an official courtroom, and the public key is mined by the public [34]. A concentrate by Chopra et al. [35] involved an elite OR activity for the watermark key, with the goal that the framework puts the watermark at a characterized area in the biometric signature design. The area is different for various pictures. This element decreases the chance of different assaults. Consequently, the vigor of the framework increments. The mutilation of the watermarked picture is controlled in view of three edge values characterized for those three classes.

To check the legitimacy, you can involve alter discovery in the watermark framework. Any adjustment of watermark information prompts picture control. In this way, by testing the respectability, the framework decides if the watermarked information has been altered or not [36].

The reversibility highlight guarantees watermark extraction and exact remaking of the host picture. Notwithstanding, for clinical imaging, the rectified picture is utilized as the host picture and the remade picture is utilized for determination [37]. In the reversible computerized watermarking technique, the framework catches the first picture and gets the watermarked picture. Then, at that point, with the assistance

of the extraction calculation, the framework recuperates the first picture and the watermark picture utilizing the mystery key.

5 Research background

Advanced picture watermarking has drawn in the consideration of specialists because of its accessibility and giving extra data. These methods shield advanced content from unapproved access and control. These strategies are required for different applications like verification, administrator validation, material security, and brand name assurance. Computerized picture watermarking methods can be ordered in light of the extent of work, sorts of reports, nature of the calculation, human discernment, and kind of use.

All advanced picture watermarking procedures rely upon the sort of area (i.e., spatial, recurrence, or crossover space), the kind of archives (text, picture, sound, or video), the idea of the calculation utilized (i.e., successive or consecutive). parallelism), human insight (for example noticeable or imperceptible), and application type (for example beginning or objective based). Summing up a portion of the new examination brings about this field, this segment breaks down various computerized picture watermarking strategies in light of the field of work. This segment will be helpful for future investigations on current watermarking techniques.

5.1 The first method - the method of expanding the difference of pairs of pixels

This procedure implants the watermark data in the host picture, as characterized by the proprietor in the spatial or transient area, utilizing different techniques including least piece (LSB), middle of the road critical piece (ISB) or fixing calculations, and range brings wide and fortitude. Calculations in light of these methods work straightforwardly on the pixels of the first picture. Watermark can be embedded by controlling pixel values in light of logo or mark data gave by Maritime et al. [17]. In the most broadly utilized plans, the forces of pixels at realized places in space address the picture, where the least piece of a specific pixel in a variety or grayscale picture is returned. Contingent upon the pixel power, the subsequent watermark might be apparent or imperceptible. We survey different ways to deal with spatial space methods that certainly stand out of specialists because of the ideal harmony between indistinctness, strength, and limit, which are the main prerequisites of any watermarking strategy. Sineq et al carried out this procedure in an article [56].

A few scientists have concentrated on varieties of the LSB method, normally connected with the spatial space. Sineq et al. [60] have created LSB procedures in view of the bitmap of discrete computerized signals (eg, sound or pictures). The bitmap that addresses the sign is a bunch of pieces that have a similar piece position

in every one of the double numbers. Most methods utilize just a single bitmap for inserting. This method deals with the least piece (for example eighth page), yet others utilize three piece pages (for example sixth and eighth piece pages) or even four digit pages (for example fifth to eighth pages). bit-planes) for inserting with satisfactory picture quality. The four least huge pieces (for example the fifth to eighth pieces of the cover picture) can be supplanted with the chose digit from the cover picture essentially by involving an OR activity in an extraordinary manner. This strategy first believers the host picture to a surge of twofold pieces, yields a zero in the implanted piece, and afterward moves the secret picture 4 pieces to one side. Then an OR activity is performed on these two (for example have and secret picture) to get the consolidated picture.

The normal spatial area checking procedure is probably going to create salt and pepper commotion outcomes. Consequently, a strategy by Sinaq et al. [64] has been proposed for variety picture watermarking in the spatial space without huge decrease in picture quality and perceptual variety change, contrasted with customary spatial area watermarking. To empower verification and additionally recuperation, watermarks are implanted in all picture blocks to guarantee higher picture quality and high heartiness against assaults. M1 and M2 guarantee that the implanted pieces make less unsettling influence the human visual framework, where M1 is the installing cover and M2 is the remuneration veil. Rectified pixels are not critical contrasted with adjoining pixels. Exploratory outcomes showed that their proposed calculation recuperates the watermark information even after bending of the most reduced pieces, and this calculation guarantees a decent PSNR esteem. Albeit the LSB method can be effectively changed, understanding how the computerized picture is changed regarding uprightness and wellbeing is a difficult errand. The LSB hash calculation checks the computerized picture utilizing a hash plot that conceals the hash capability. One review inserted the LSB hash code to safeguard the first record and extricated the implanted hash code to deliver a result document that gave off an impression of being equivalent to the first record. For this situation, the installed watermark utilized for information extraction is undetectable [65]. Be that as it may, LSB strategies can be effectively carried out, and thus, the related computational intricacy might be diminished [8].

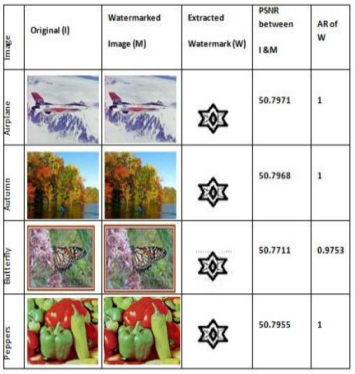


Fig 3 of the results obtained in reference [19]

5.2 The second method - the method of expanding the difference in groups of three pixels

In this method, in order to increase the embedding capacity, we use groups of three pixels. The algorithm embeds two bits in all three groups of three. Therefore, this method has a maximum embedding capacity equal to 2.3 bpp, and compared to Tian's bpp method, the capacity is slightly improved.

Associates in [69] showed the strength and shortcoming of advanced picture watermarking strategies by characterizing PSNR and NCC limit values. The examined watermarking method implanted four watermarks in the ISB of six grayscale picture documents individually by supplanting the pixels of the first picture with new pixels and keeping them near the first pixel esteems at the same time. Their proposed calculation in view of PSNR and NCC values showed better heartiness against some normal picture handling activities, for example, sifting, pressure, clamor and obscure. Vigor against mathematical change assaults, like scaling and turn, where pixel forces are not impacted by modified areas isn't corrupted. Consequently, to expand the power of messages against different assaults and to oppose mathematical changes (like scaling, cutting, and separating), ISB procedures can be utilized rather than LSB methods, where the mystery message can be implanted in a bitmap. (Or bit pages) [70].

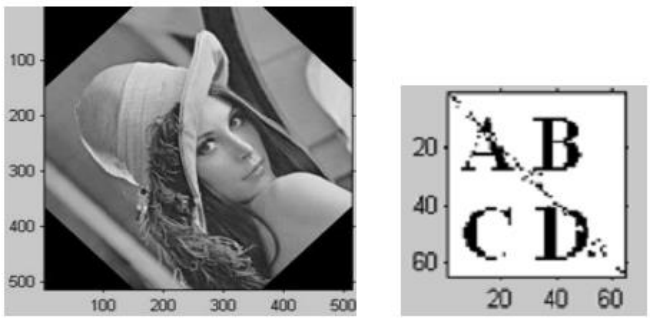
Embedding operation

The direct conversion for the ternary category is defined based on the equation (27-2):

$$u_1 = v_0 - \left\lfloor \frac{v_1 + v_2}{N} \right\rfloor$$
$$u_0 = v_2 + u_1 \qquad (2\text{-}28)$$
$$u_2 = v_1 + u_1$$

5.3 The third method - Reversible cryptography based on two-dimensional difference expansion

By using this method, the embedding capacity increases due to the reduction of the embedding map size. Interwoven is a semi irregular measurable cycle that is imperceptibly implanted in a unique picture utilizing extra example encoding by a Gaussian circulation. Two fixes An and B are chosen pseudo-haphazardly, and the picture information of the primary fix (A) is blurred, while those in B are obscured. Rashid et al. [71] showed that fixing techniques show better vigor against most extreme non-mathematical changes of the picture and this interaction is autonomous of the substance of the first picture. For this situation, vigor can be expanded by relative coding, highlight identification, or both, and the code can be lost by scaling, interpretation, or revolution prior to disentangling. Albeit unprejudiced fixing is impervious to cutting, it decreases precision. A pseudo-irregular piece stream is created by choosing sets of pixels from the first picture. A touch of data is encoded two by two, where d addresses the contrast between two pixels. The encoding is 0 for $d < 0$ and pixels are traded for $d > 0$. The following pair can advance in the event that d is equivalent to 0 or more prominent than a predefined edge [72]. Thusly, the brilliance can be expanded by one unit at one point and diminished at another point. This technique is appropriate for enormous areas of arbitrary surface, yet not for text pictures. A region of the arbitrary surface example in the picture is duplicated to a region of the picture with a similar surface. Each tissue area is recuperated through autocorrelation [73]. In a concentrate by Touhidi et al. [74], a summed up piecing calculation comprising of gradual and multiplicative lumping was proposed. This technique involves factual information for watermark installing and location. To recognize the watermark information, this technique utilizes relocation plan and scale change plot. Their proposed technique is vigorous against pressure assaults. Notwithstanding, the vigor against different assaults in the sharding technique is extremely high. A limited quantity of information can be covered up [75]. The watermark can be implanted in a picture utilizing extra example encryption, and the watermark can be removed utilizing a mystery key relating to the unscrambling calculation.



(a) (b)

Fig 4 of the results obtained in reference [29]

For an image of size I, we first perform horizontal division and obtain p. In horizontal division, pairs of pixels are selected from left to right, and p is calculated using equations (2-31) and (2-32).

$$P_{i,j} = \frac{I_{i,2j} + I_{i,2j+1}}{2} \quad \text{when } 0 \le j \le \frac{n}{2} \tag{2-31}$$

$$P_{i,j} = \frac{I_{i,2\left(j-\frac{n}{2}\right)} - I_{i,2\left(j-\frac{n}{2}\right)+1}}{2} \quad when\ \frac{n}{2} \le j < n \tag{2-32}$$

Now we use the image p for vertical division. In vertical division, we consider pairs of pixels vertically and from top to bottom, and then calculate the image :(2-34) Q using the relations (2-33) and

$$Q_{i,j} = \frac{P_{2i,j} + P_{2i+1,j}}{2} \quad when\ 0 \le i < \frac{n}{2} \tag{2-33}$$

$$Q_{i,j} = \frac{P_{2\left(i-\frac{n}{2}\right),j} - P_{2\left(i-\frac{n}{2}\right)+1,j}}{2} \quad when\ \frac{n}{2} \le i < n \tag{2-34}$$

Table 2 comparison of previous researches

Watermarking method	suggested method	year of publication	Author Name
The method of expanding the difference of pairs of pixels	Analytical study of a new color image encoding method based on chaos system and color codes	2021	Naval and colleagues [17]

The method of expanding the difference of pairs of pixels	Medical image watermarking of multimedia systems and applications	2017	Sink et al. [56]
The method of expanding the difference of pairs of pixels	Multiple watermarking technique for securing online social network content using back propagation neural network	2016	Sink et al. [60]
The method of expanding the difference of pairs of pixels	Digital watermark design for copyright protection and tamper detection	2019	Hsu et al. [67]
The method of expanding the difference of pairs of pixels	Blind 3D mesh watermarking based on mesh saliency and wavelet transform for copyright protection	2019	Hamidi et al. [68]
The method of expanding the difference in groups of three pixels	A new reversible watermarking scheme based on SHA3 for copyright protection and integrity of satellite images	2019	Kenho et al. [69]
Reversible cryptography based on two-dimensional difference expansion	Digital Watermarking Applications and Techniques: A Short Review	2016	Rashid et al. [71]

6 Proposed watermark algorithm

Violet's algorithm is commonly applied to transform domain images. This causes conventional algorithms to respond well and not be fragile in case of an attack in this way, which is often in this field. In the proposed method, to strengthen the watermark algorithm in the images, random forest algorithm and refrigeration are used in the field of selecting the allowed areas for information hiding. Figure (3-1) shows the flowchart of the proposed method:

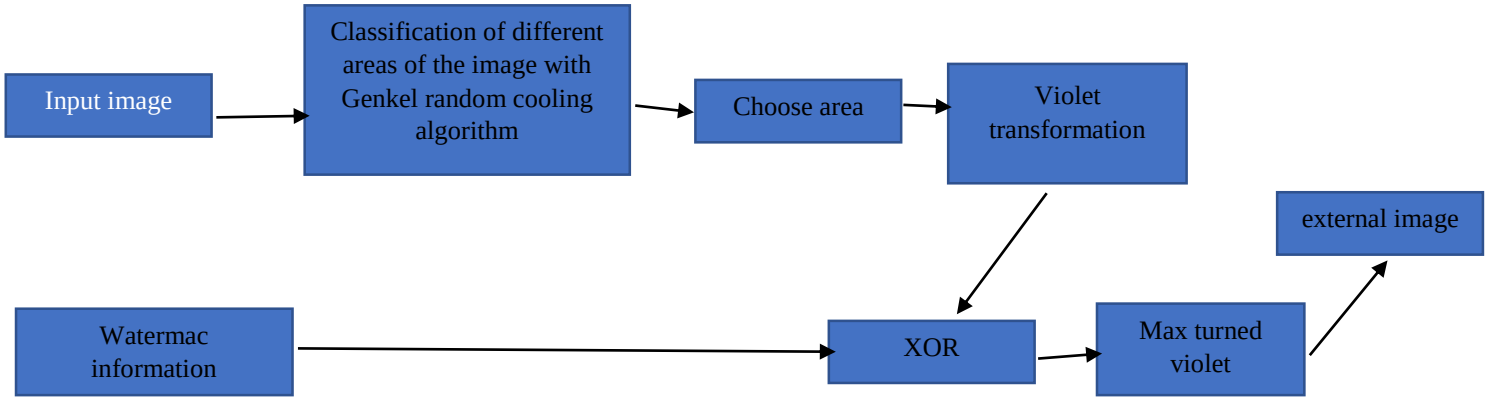


Fig 5 flowchart of the proposed method

The transformation used in this method is the violet transformation, which is applied to an area of the input image that is cut to insert the watermark information. This cropped area is called a region of interest or ROI. Watermarking calculations that are not secure can't be applied to copyright assurance, information confirmation, fingerprinting, and advanced content following. Subsequently, security is a significant worry in computerized picture watermarking methods. Security can be checked by different encryption techniques, where the key decides the degree of safety. A few strategies, for example, mayhem based strategies, discrete cosine change (DCT), and calculated map-based encryption procedures, have been utilized to guarantee the security and privacy of the inserted watermark [24]. The security of utilitarian attractive reverberation imaging (fMRI) pictures is significant on the grounds that they connect with cerebrum movement. A watermarking strategy to guarantee the honesty and precision of fMRI pictures has been proposed [25], where a delicate reversible watermarking plan was acquainted with distinguish fMRI pictures that are liberated from any curios. This plan doesn't rely upon the utilization of outer metadata. In [26], pseudo-irregular double successions were utilized for watermark encryption prior to implanting, which expanded the security of the watermark calculation. Security prerequisites can be applied to telemedicine, computerized imaging, media communications, sight and sound information, and so on.

6.1 Implementation of the proposed method

In the proposed method, as shown in the figure below, it uses the violet transformation, which is applied to the base image. The applied violet transform can be applied in several levels (sub-bands), but here we will use only one transform level. The wavelet used in this conversion can be selected from the available wavelets. An important point used in this work is the use of int2int wavelet

transformation, which will be completely reversible and practical at the level of digital implementation. Because in many conversions, storing information and retrieving them due to the conversion from integer to real number will have loss [38] existing discrete wavelet conversions will not be exactly reversible, for this reason and to solve this problem, int2int wavelet conversion in Invented in 1998 [39] the wavelet used in this one-to-one conversion is called Lazy Lifting Scheme. Suppose k(j), M(j) are two sets of even and odd events, then:

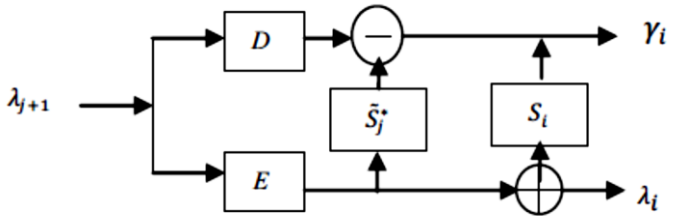


Fig 6 Violet int2int conversion with Lazy Lifting Scheme

This feature is an important advantage in watermark algorithms. By comparing the PSNR of these two images, it can be seen that the proposed method has a higher score 17

in this field, so that the PSNR of the proposed method is 49.68, and this number is 49.32 for the previous method.

Fig 7 the allowed areas for information insertion in the overlay image obtained by random forest algorithm and refrigeration

Fig 8 comparing the output watermarked images using the new method and the previous method

In an overview, Table (4-1) shows a comparison between the watermark image extraction results between our proposed method and the method before optimization. As can be seen visually, the output image of the proposed method is better than the other one against the majority of attacks:

The following table shows the PSNR parameter for the mentioned attacks for the extracted watermark image. It is worth noting that the concept of Inf expressed in this table means that the extracted image is similar to the original logo image. From the numbers in the table, it is clear that the proposed method is relatively more resistant to the jpeg compression attack and is better than the previous method.

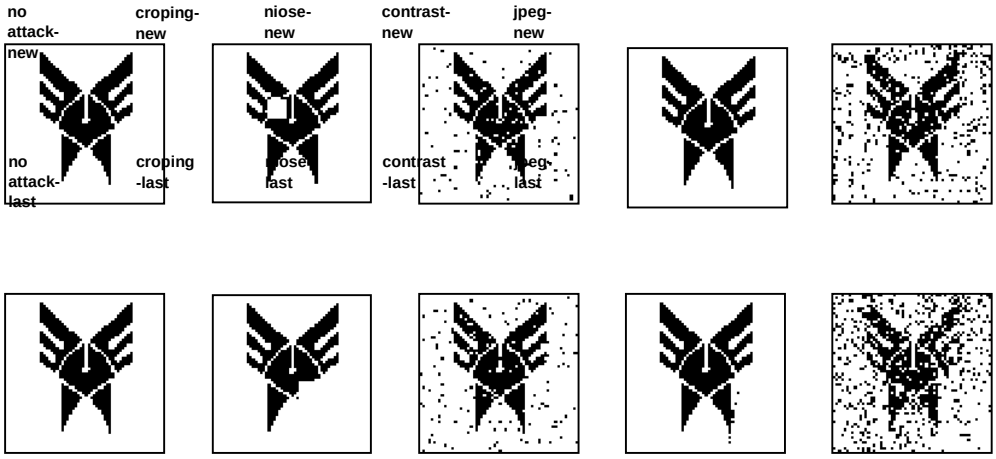


Fig 9 comparing the extracted watermark image between the proposed method (first line) and the method before optimization (second line) against different attacks

Type of attack	no attack	cropping	niose	contrast	jpeg
suggested method	*Inf*	*66.53*	*62.62*	*Inf*	*58.07*
method [65]	*Inf*	*64.34*	*62.35*	*74.66*	*56.30*

Table 3 comparing the results of the PSNR parameter of the image extracted from different attacks in the image of Figure 2-4

For another image below, the same two algorithms were implemented again and the following results were obtained. Like the previous image, this image has better results for the proposed algorithm

Fig 10 Cover image of the test case and comparison of output watermarked images using the new method and the previous method

Table 4 comparing the results of the PSNR parameter of the image extracted from different attacks in the image of Figure 12-4

Type of attack	no attack	cropping	niose	contrast	jpeg
suggested method	*Inf*	*66.61*	*62.02*	*Inf*	*57.53*
method [65]	*Inf*	*64.34*	*62.52*	*61.23*	*55.31*

It is interesting that by applying several images in this way and statistical analysis, he gave a general conclusion of the proposed algorithm. Therefore, the images of the following collection were watermarked according to the suggested method. These images, which are a total of 10 images, which are usually standard images in the field of digital image processing, all of which are accessible in different formats

and sizes on the Internet (Figure 13-4), are again selected from standard image processing images for completeness. acceptable for the final result

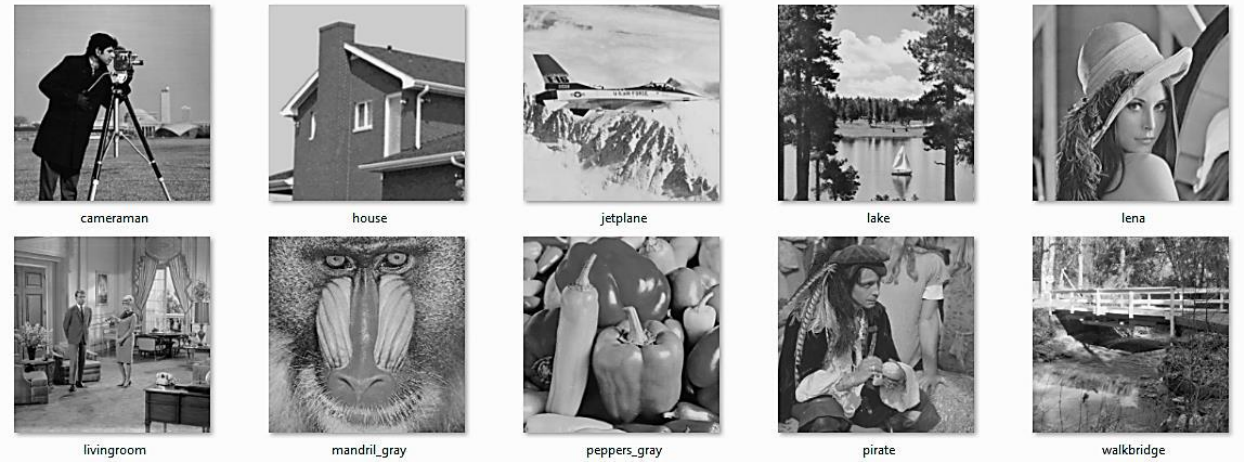


Fig 11 test data set images

The following table shows the improvement value of the PSNR parameter for the watermarked image itself and the mentioned attacks for the extracted image on the database images. The negative sign means to decrease the PSNR parameter. The houses marked in red do not follow the general improvement procedure and in them we have a decrease in PSNR. The first image (Cameraman) in the table below is not in a good condition, as well as the sixth image (livingroom).

Table 5 comparing the results of the PSNR parameter of the overlay image and the extracted image under different attacks in the database image Figure 13-4

	cover	cropping	niose	contrast	Jpeg
Cameraman	**+2.74**	**-0.47**	**-0.9**	**>>0**	**+1.9**
house	**+ 2.63**	**+2.54**	**-0.92**	**<<0**	**+ 2.59**
jetplane	**+1.41**	**+2.27**	**+0.23**	**<<0**	**+ 2.22**
lake	**+ 0.66**	**+ 2.54**	**+ 0.09**	**<<0**	**-0.88**
lena	**+0.36**	**+2.19**	**+0.25**	**<<0**	**+ 1.77**
livingroom	**+ 1.48**	**+1.71**	**-0.77**	**-0.79**	**+3.19**
mandril	**+1.08**	**+2.63**	**+0.28**	**<<0**	**+ 0.52**
peppers	**+ 1.86**	**+ 2.62**	**+ 0.24**	**+ 15.32**	**+ 0.08**
pirate	**+ 0.51**	**+2.63**	**+0.25**	**<<0**	**+1.83**
walkbridge	**+2.55**	**+2.54**	**+0.53**	**+11.1**	**+1.16**

7 Conclusion

According to the results, by comparing the PSNR of two hidden images and the base image, it can be seen that the proposed method has a very good score, so that the PSNR of the proposed method is 197.7. On the other hand, I was resistant to check the proposed algorithm in the effect of various attacks, simulations were carried out that the attacks we used are in the form of 4 attacks: cutting the image, adding noise, changing the contrast and finally applying the JPEG compression algorithm on the image. . The first attack that was mentioned was the image cropping attack. If this attack happens exactly in the place where we have chosen to insert information, our information will be lost, but if it happens in another place, the results will not lead to the deletion of information. The results show the good resistance of this method in maintaining the inserted information.

Also, by implementing the proposed method on the database images, the watermarked image by the proposed method is on average 1.5280 times more than the previous method that uses the Violet algorithm without the random forest algorithm and refrigeration. Also, the proposed method is on average 2.12 dB better against the image clipping attack, 0.07 dB worse against the image noise attack (this value is very low), significantly better against the contrast attack, and finally 1.43 dB better for the compression attack. It is made by jpeg method. In a summary, it can be said that apart from improving the quality of the output watermark image, the proposed method has a better response against image cropping and compression attacks using the jpeg method. Nowadays, information can be easily reproduced due to the interactive and digital communication of multimedia data. This makes digital image watermarking an important research field. Digital image watermarking using various techniques has been used as an important tool for image authentication, integrity verification, tamper detection, copyright protection and digital security of an image. In this study, we reviewed the most prevalent watermarking techniques. Through this study, it can be concluded that DWT is a quality and robust technique for image watermarking due to its multiple resolution features.Robustness, obscurity and capacity are the basic requirements in designing an efficient watermarking system. However, it is almost impossible to achieve all these requirements simultaneously. Therefore, a good trade-off between these three requirements should be maintained. However, security remains a major challenge in digital image watermarking technologies, and the adaptation of IoT and blockchain-based authentication schemes poses a challenge for researchers. Therefore, future work can be extended by combining different techniques in different domains to meet the above three important requirements. Furthermore, to improve robustness along with security, researchers should focus on developing new and advanced techniques. Some things can be suggested below that will be useful for future works:

• Use other transformations such as curvelet

• Combining different techniques in different areas to meet the three requirements of robustness, imperceptibility and capacity

• Solutions for adapting authentication plans based on the Internet of Things and Blockchain

• Improving the robustness along with the security of different algorithms in content-based information embedding

8 Reference

1. Banday, S. A., Pandit, M. K., & Khan, A. (2021). Securing medical images via a texture and chaotic key framework. In *Multimedia Security* (pp. 3-24). Springer, Singapore.
2. Evsutin, O., Kokurina, A., Meshcheryakov, R., & Shumskaya, O. (2018). The adaptive algorithm of information unmistakable embedding into digital images based on the discrete Fourier transformation. *Multimedia Tools and Applications*, *77*(21), 28567-28599.
3. Liu, Z. L., & Pun, C. M. (2019). Reversible image reconstruction for reversible data hiding in encrypted images. *Signal Processing*, *161*, 50-62.
4. Singh, S., & Jung, K. H. (2022). Special issue on emerging technologies for information hiding and forensics in multimedia systems. *Multimedia Tools and Applications*, 1-8.
5. Chang, T. J., Pan, I. H., Huang, P. S., & Hu, C. H. (2019). A robust DCT-2DLDA watermark for color images. *Multimedia Tools and Applications*, *78*(7), 9169-9191.
6. Wu, H. T., Cao, X., Jia, R., & Cheung, Y. M. (2022). Reversible Data Hiding with Brightness Preserving Contrast Enhancement by Two-dimensional Histogram Modification. *IEEE Transactions on Circuits and Systems for Video Technology*.
7. Dong, T., Hong, Z., & Yin, Z. (2018, December). High-Fidelity Reversible Data Hiding in JPEG Images Based on Two-Dimensional Histogram. In *International Conference on Security with Intelligent Computing and Big-data Services* (pp. 116-128). Springer, Cham.
8. El Khoury, K., Fockedey, M., Brion, E., & Macq, B. (2021). Improved 3D U-Net robustness against JPEG 2000 compression for male pelvic organ segmentation in radiotherapy. *Journal of Medical Imaging*, *8*(4), 041207.
9. Sharma, S., Zou, J. J., & Fang, G. (2022). A dual watermarking scheme for identity protection. *Multimedia Tools and Applications*, 1-30.

10. Smith, M. R., Khan, S., & Curiel, L. (2022). Investigation of hardware and software techniques to enhance the characteristics of focused ultrasound (FUS) spectra. *Physics in Medicine & Biology*.
11. Banday, S. A., & Pandit, M. K. (2021). Texture maps and chaotic maps framework for secure medical image transmission. *Multimedia Tools and Applications*, *80*(12), 17667-17683.
12. Wang, C., Wang, S., Xia, Z., Li, Q., Ma, B., Li, J., ... & Shi, Y. Q. (2021). Medical image super-resolution via deep residual neural network in the shearlet domain. *Multimedia Tools and Applications*, *80*(17), 26637-26655.
13. Jabarulla, M. Y., & Lee, H. N. (2020). Blockchain-based distributed patient-centric image management system. *Applied Sciences*, *11*(1), 196.
14. Yin, X., Lu, W., Zhang, J., & Liu, W. (2020). Reversible data hiding in halftone images based on minimizing the visual distortion of pixels flipping. *Signal Processing*, *173*, 107605.
15. Mo, L., Zhu, L., Ma, J., Wang, D., & Wang, H. (2021). MDRSteg: large-capacity image steganography based on multi-scale dilated ResNet and combined chi-square distance loss. *Journal of Electronic Imaging*, *30*(1), 013018.
16. Samanta, K., & Joseph, J. (2021). An overview of structured illumination microscopy: recent advances and perspectives. *Journal of Optics*.
17. Kanwal, S., Inam, S., Cheikhrouhou, O., Mahnoor, K., Zaguia, A., & Hamam, H. (2021). Analytic study of a novel color image encryption method based on the chaos system and color codes. *Complexity*, *2021*.
18. GEORGIEVA, A., PANAYOTOVA, K., & IVANOV, Z. (2019). Obtaining Nanostructured Catalyst Systems and Study of Catalytic Efficiency. *Oxidation Communications*, *42*(2), 121-131.
19. Wu, J., Liu, X., Liu, X., Tang, Z., Huang, Z., Lin, W., ... & Yi, G. (2022). A High-Security mutual authentication system based on structural color-based physical unclonable functions labels. *Chemical Engineering Journal*, *439*, 135601.
20. Lakshmi, H. R., & Borra, S. (2021). Difference expansion based reversible watermarking algorithms for copyright protection of images: state-of-the-art and challenges. *International Journal of Speech Technology*, *24*(4), 823-852.
21. Tao, H.; Chongmin, L.; Zain, J.M.; Abdalla, A.N. Hearty Picture Watermarking Hypotheses and Strategies: A Survey. J. Appl. Res. Technol. 2014, 12, 122-138.
22. Zhang, Y. Computerized Watermarking Innovation: A Survey. In Procedures of the ETP Global Gathering on Future PC and Correspondence, Wuhan, China,6–7 June 2009; pp. 250–252.

23. 23. Digital Watermarking and Steganography, Second Edition; The Morgan Kaufmann Series in Multimedia Information and Systems: Burlington, Massachusetts, 2008; Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T..
24. A review of digital watermarking techniques for image security was conducted by Mohanarathinam, A., Kamalraj, S., Venkatesan, G.P., Ravi, R.V., and Manikandababu, C.S. Human-Computer J. Ambient Intelligence 2019, 1–9.
25. Cox, I.J. and Miller, M.L. "Perceptual modeling is important and watermarking is reviewed." 1997 SPIE Proc. 3016.
26. . A Secure and Adaptive Holographic Image Watermarking System by Yu, C., Li, X., Chen, X., and Li, J. 2019; Entropy, 21, 460.
27. . Image Digital Watermarking: A Survey, Kumar, V.A.; Rao, C.H.S. ; Dharmaraj, C. International Journal of Advanced Management Technology and Engineering Science, 2018, 8, 127–143
28. Jaynes, E.T. Prior probabilities. IEEE Trans. Syst. Sci. Cybern. 1968, 4, 227–241.
29. Refregier, P.; Javidi, B. Optical Image Encryption based on Input Plane and Fourier Plane Random Encoding. Opt. Lett. 1995, 20, 767–769.
30. . Wu, C.; Ko, J.; Rzasa, J.R.; Paulson, D.A.; Davis, C.C. Stage and Adequacy Shaft Molding with Two Deformable Mirrors Carrying out Info Plane and Fourier Plane Stage Adjustments. Appl. Pick. 2018, 57, 2337-2345.
31. Pun, C.M. High Limit and Hearty Advanced Picture Watermarking. In Procedures of the fifth Worldwide Joint Meeting on INC, IMS and IDC, Seoul, South Korea, 25-27 August 2009; pp. 1457-1461.
32. Yang, H.M.; Liang, Y.Q.; Wang, X.D.; Ji, S.J. A DWT-Based Assessment Strategy for Impalpability of Watermark in Watermarked Variety Picture. In Procedures of the 2007 Worldwide Gathering on Wavelet Examination and Example Acknowledgment, Beijing, China, 2-4 November 2007; pp. 198-203.
33. Zhang, H.; Wang, C.; Zhou, X. A Hearty Picture Watermarking Plan In light of SVD in the Spatial Space. Future Web 2017, 9, 45.
34. 34. Takore, T.T.; Kumar, P.R.; Devi, G.L. Another Powerful and Impalpable Picture Watermarking Plan In view of Crossover Change and PSO. Int. J. Intell. Syst. Appl. 2018, 11, 50-63.
35. Liu, J.; He, X. A Survey Concentrate on Computerized Watermarking. In Procedures of the first Global Meeting on Data and Correspondence Advances, ICICT, Karachi, Pakistan, 27-28 August 2005; pp. 337-341.Olanrewaju, R.F. Development of Intelligent Digital Watermarking via Safe Region. Ph.D. Thesis, Kulliyyah of Engineering, International Islamic University Malaysia, Selangor, Malaysia, 2011.

36. Yadav, U.; Sharma, J.P.; Sharma, D.; Sharma, P.K. Different Watermarking Strategies and its Applications: A Survey. Int. J. Sci. Eng. Res. 2014, 5, 1288-1294.
37. Cvejic, N. Calculations for Sound Watermarking and Steganography. Expert's Proposition, Division of Electrical and Data Designing, College of Oulu, Oulu, Finland, 2004.
38. Zhang, H.; Wang, C.; Zhou, X. Delicate Watermarking for Picture Validation. Utilizing the Quality of SVD. Calculations 2017, 10, 27.
39. Sang, J.; Alam, M.S. Delicacy and Power of Double Stage Just Channel Based Delicate/Semi delicate Advanced Picture Watermarking. IEEE Trans. Instrum. Meas. 2008, 57, 595-606.
40. Zhang, Y.; Wang, C.; Wang, X.; Wang, M. Include Based Picture Watermarking Calculation Involving SVD and APBT for Copyright Security. Future Web 2017, 9, 13.
41. Zhou, X.; Zhang, H.; Wang, C. A Hearty Picture Watermarking Method In light of DWT, APDCBT, and SVD. Balance 2018, 10, 77.
42. Loani, N.A.; Hurrahi, N.N.; Parah, S.A.; Lee, J.W.; Sheikhi, J.A.; MohiuddinBhat, G. Secure and Powerful Advanced Picture Watermarking Utilizing Coefficient Differencing and Tumultuous Encryption. IEEE Access 2018, 6, 19876-19897.
43. Castiglione, A.; Pizzolante, R.; Palmieri, F.; Masucci, B.; Carpentieri, B.; De Santis, A. On-Board Organization Autonomous Security of Practical Attractive Reverberation Pictures. ACM Trans. Install. Comput. Syst. 2017, 16, 1-15.
44. . Wang, C.; Zhang, H.; Zhou, X. A Self-Recuperation Delicate Picture Watermarking with Variable Watermark Limit. Appl. Sci. 2018, 8, 548.
45. Zhang, F.; Zhang, H. Computerized Watermarking Limit and Dependability. In Procedures of the IEEE Global Meeting on web based business Innovation, San Diego, CA, USA, 9 July 2004; pp. 295-298.
46. Katti, S.J.; Namuduri, V.R.; Namuduri, K.R. A Down to earth Approach for Assessing the Limit of Watermarking Channel. In Procedures of the Global Gathering on Astute Detecting and Data Handling, Chennai, India, 4-7 January 2005; pp. 193-198.
47. Kavitha, K.J.; Shan, B.P. Execution of DWM for Clinical Pictures involving IWT and QR Code as a Watermark. In Procedures of the IEEE Meeting on Arising Gadgets and Brilliant Frameworks, Tiruchengode, India, 3-4 Walk 2017; pp. 252-255.
48. Pizzolante, R.; Castiglione, A.; Carpentieri, B. Assurance of Microscopy Pictures through Computerized Watermarking Strategies. In Procedures of the Global Gathering on Astute Systems administration and Cooperative Frameworks, Salerno, Italy, 10-12 September 2014; pp. 65-72.

49. . Ling, H.- C.; Phan, R.C.- W.; Heng, S.- H. Remark on Powerful Visually impaired Picture Watermarking Plan In light of Repetitive Discrete Wavelet Change and Solitary Worth Disintegration. AEU-Int. J. Electron. Commun. 2013, 60, 894-897.
50. Goos, G.; Hartmanis, J.; Van Leeuwen, J. Distributed computing and Security. In Procedures of the fourth Worldwide Gathering, ICCCS, Haikou, China, 8-10 June 2018; pp. 691-697.P'erez-Freire, L.; Na, P.C.; Ramon, J.; Troncoso-Pastoriza, J.R.; Gonzalez, F.P. Watermarking Security: A Survey. In Transactions on Data Hiding and Multimedia Security; Lecture Notes in Computer Science: Berlin/Heidelberg, Germany, 2006; pp. 41–72.
51. . Bruce, A.M. A Survey of Computerized Watermarking. Accessible on the web: https: //pdfs.semanticscholar.org/d6eb/c1a3e1676df1b5a32033417215e8da096ac4.pdf (got to on 16 February 2020).
52. Chopra, J.; Kumar, A.; Kumar, A.; Marwaha, A. A Productive Watermarking for Safeguarding Mark Biometric Layout. In Procedures of the fifth Worldwide Meeting on Signal Handling and Coordinated Organizations (Twist), Noida, India, 22-23 February 2018; pp. 413-418.
53. Singh, A.K.; Kumar, B.; Singh, G.; Mohan, A. Clinical Picture Watermarking. Sight and sound Frameworks and Applications; Springer: Berlin/Heidelberg, Germany, 2017.
54. Qasim, A.F.; Meziane, F.; Aspin, R. Advanced watermarking: Pertinence for Creating Confidence in Clinical Imaging Work processes Cutting edge Audit. Comput. Sci. Fire up. 2018, 27, 45-60.
55. De Vleeschouwer, C.; Delaigle, J.; Macq, B. Imperceptibility and Application Functionalities in Perceptual Watermarking-An Outline. Proc. IEEE 2002, 90, 64-77.
56. Merrad, A. Execution of a Biometric Discourse Watermarking In view of Wavelet Change. Ph.D. Theory, Ziane Achour College of Djelfa, Djefa, Algeria, 2019.
57. Singh, A.K.; Kumar, B.; Singh, S.K.; Ghrera, S.P.; Mohan, A. Numerous Watermarking Method for Getting On the web Interpersonal organization Items Utilizing Back Proliferation Brain Organization. Future Gener. Comput. Syst. 2016, 86, 926-939.
58. Zear, A.; Singh, A.K.; Kumar, P. A Proposed Secure Various Watermarking Strategy In light of DWT, DCT and SVD for Application in Medication. Multimed Apparatuses Appl. 2016, 77, 4863-4882.
59. Phadikar, A.; Jana, P.; Mandal, H. Reversible Information Stowing away for DICOM Picture Utilizing Lifting and Companding. Cryptography 2019, 3, 21.

60. Yusof, Y.; Khalifa, O.O. Advanced Watermarking for Computerized Pictures utilizing Wavelet Change. In Procedures of the IEEE Worldwide Gathering on Broadcast communications and Malaysia Global Meeting on Correspondences, Penang, Malaysia, 14-17 May 2007; pp. 665-669.
61. Singh, V. Computerized Watermarking: An Instructional exercise. Accessible on the web: http: //www.cyberjournals.com/Papers/Jan2011/02.pdf (got to on 16 February 2020).
62. Agbaje, M.; Olugbenga Awodele, O.; Idowu, S.A. Broadcast Checking and Applications. J. Telecommun. 2012, 7, 11-16.
63. Kaur, E.J.; Kaur, E.K. Computerized Watermark: A Review. Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2012, 2, 159-163.
64. Hsu, C.S.; Tu, S.F. Advanced Watermarking Plan for Copyright Security and Altering Discovery. Int. J. Inf. Technol. Secur. 2019, 11, 107-119.
65. Hamidi, M.; Chetouani, A.; El Haziti, M.; El Hassouni, M.; Cherifi, H. Blind Hearty 3D Cross section Watermarking In view of Lattice Saliency and Wavelet Change for Copyright Assurance. Data 2019, 10, 67.
66. Kunhu, A.; Al Mansoori, S.; Al-Ahmad, H. An Original Reversible Watermarking Plan In light of SHA3 for Copyright Security and Trustworthiness of Satellite Symbolism. Int. J. Comput. Sci. Netw. Secur. 2019, 19, 92-102.
67. Furon, T. An Overview of Watermarking Security; Global Studio on Computerized Watermarking: Siena, Italy, 2005; pp. 201-215.
68. Rashid, A. Computerized Watermarking Applications and Procedures: A Concise Survey. Int. J. Comput. Appl. Technol. Res. 2016, 5, 147-150.
69. Adnan, W.A.W.; Hitarn, S.; Abdul-Karim, S.; Tamjis, M.R. A Survey of Picture Watermarking. In Procedures of the Understudy Gathering on Innovative work, Putrajaya, Malaysia, 25-26 August 2003; pp. 381-384.
70. Mahajan, J.R.; Patil, N.N. Alpha Channel for Honesty Check utilizing Computerized Mark on Reversible Watermarking QR. In Procedures of the 2015 Worldwide Gathering on Figuring Correspondence Control and Computerization, Pune, India, 26-27 February 2015; pp. 602-606.