Journal of Engineering Sciences
Vol 10, Issue 12, Dec /2019
ISSN NO:0377-9254

BLIND DUAL WATERMARKING FOR COLOR IMAGES USING MATLAB

[1]S.HARITHA, [2]I.RAJASEKHAR
[1]M.Tech Student, [2]HOD & Associate Professor ,
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING,
SHRI SHIRDI SAI INSTITUTE OF SCIENCE AND ENGINEERING,
ANANTAPURAMU, ANDHRA PRADESH

Abstract: This paper presents a blind dual watermarking mechanism for digital color images in which invisible robust watermarks are embedded for copyright protection and fragile watermarks are embedded for image authentication. For the purpose of copyright protection, the first watermark is embedded using the discrete wavelet transform in YCbCr color space, and it can be extracted blindly without access to the host image. However, fragile watermarking is based on an improved least significant bits' replacement approach in RGB components for image authentication. The authenticity and integrity of a suspicious image can be verified blindly without the host image and the original watermark.

The combination of robust and fragile watermarking makes the **proposed mechanism** suitable for protecting valuable original images. The experimental results indicated that the proposed watermarking mechanism can withstand various processing attacks and accurately locate the tampered area of an image.

I.INTRODUCTION:

In a few works, information stowing away and encryption are pointed with a basic way. For instance, a piece of cover information is utilized for conveying extra information and the rest information are scrambled for security insurance [8, 9]. On the other hand, the extra information is implanted into an information space that is perpetual to encryption activities [10]. In another sort of the works, information implanting is performed in encoded area, and an approved collector can recuperate the first plaintext cover picture and concentrate the inserted information. This method is named as reversible information covering up in scrambled pictures (RDHEI). In a few situations, for safely sharing mystery pictures, a substance proprietor may encode the pictures previously transmission, and a substandard partner or a channel head wants to affix some extra messages, for example, the source data, picture documentations or confirmation information, inside the scrambled pictures however he doesn't know the picture content. For instance, when therapeutic pictures have been encoded for securing the patient protection, a database director may plan to implant the individual data into the relating scrambled pictures. Here, it might be cheerful that the first substance can be recouped with no blunder after unscrambling and recover of extra message at beneficiary side.

The execution of RDHEI can be additionally enhanced by presenting a usage arrange [12] or a flipping proportion [13]. In [14], each extra piece is implanted into a square of information encoded by the AES. Despite the fact that the computational multifaceted nature is higher, the foundation of mystery key through a protected channel between the sender and the collector is unnecessary. With the strategy in [20], every pixel is separated into two sections: a considerably number and a bit, and the two sections are encoded utilizing Parlier instrument [21], individually. At that point, the cipher text estimations of the second parts of two adjoining pixels are altered to suit an extra piece. Due to the homomorphism property of the cryptosystem, the implanted piece can be separated by looking at the relating unscrambled values on beneficiary side. Actually, the homomorphism property might be additionally abused to actualize flag handling in scrambled area [22, 23, and 24]. For recuperating the first plaintext picture, a converse activity to recover the second piece of every pixel in plaintext area is required, and after that two unscrambled parts of every pixel ought to be revamped as a pixel. With the consolidated strategy, a beneficiary may remove a piece of implanted information before unscrambling, and concentrate another piece of installed information and recoup the first plaintext picture after decoding.

"Security" is of prime worry as the prepared picture ought not to be spilled or outsider got to in any capacity and to keep it secret if necessary. It is arranged into two sorts Steganography and steganalysis. Steganography depends on installed procedure and steganalys depends on identification system. Steganography shrouds pictures in the front of something unique. PEG is the organization normally utilized for covering up as it is the generally utilized record in web. Records are compacted and encoded again to up the level of mystery.

1.1 Basics of Image Data Hiding

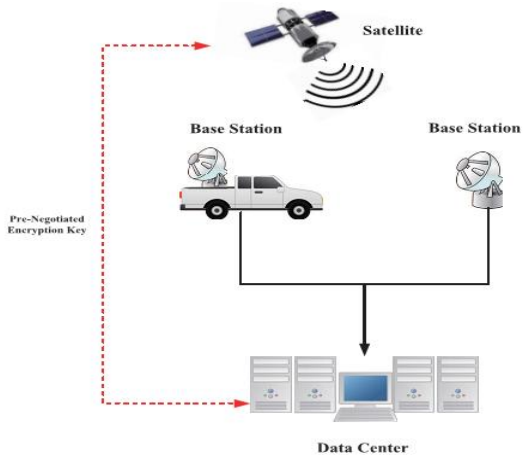


Fig. 1 Image data hiding

In any case, the implanting limit of this sort of strategy is fairly constrained and the brought about contortion on the watermarked picture is serious. Histogram moving based system, at first planned by Ni et al, is another class of approach accomplishing better installing execution through moving of the histogram of some picture highlights. The most recent contrast development based plans and the enhanced forecast mistake extension based techniques were appeared to have the capacity to offer the best in class capacity– contortion execution.

These days with the development in the data innovation, there has opened new open doors in logical and business applications. Nonetheless, this advancement has caused a great deal of significant issues including hacking, duplications and noxious use of computerized in-arrangement. Steganography which alludes to the mystery correspondence endeavors to address these developing concerns. A mystery message is implanted into a host or cover flag (unique sound, picture or video information) by somewhat adjusting its substance that outcomes in a watermarked or steno flag. The turn around task is called extraction. Note that Steganography applications have no an incentive for the host flag, which assumes the part of a fake to cover the specific nearness of correspondence. All things considered, non-reversible plans are utilized, in which us the mystery message is separated. Be that as it may, there are various different applications, which require both the cover picture and the mystery message at the yield and depend on computationally overwhelming reversible or lossless information concealing methods. This gathering of uses otherwise known as advanced watermarking related nearly to the cover flag. The mystery message involves the extra information about the flag, which builds its down to earth esteem, be that as it may, presents some measure of bending. Note that a few applications can't manage any mutilation, e.g. medicinal symbolism, where each piece disconnected arrangement is imperative.

Fig .2 Data Embedding Term

1.2 Data Hiding Main Terms And Notions

Among the lossless methods of information installing there are two basic spaces of activity: spatial and recurrence. Spatial systems are portrayed by the implanting of messages into the minimum huge bits (LSBs) of picture pixels, while in recurrence strategies the message is installed after a specific change is performed by altering recurrence coefficients of the cover picture.

As of late, the exploration on flag handling over encoded area has increased expanding consideration, principally determined by the requirements from distributed computing stages and different security saving applications. This has set off the examination of installing extra information in the scrambled pictures in a reversible design. In numerous down to earth situations, e.g., secure remote detecting and distributed computing, the gatherings that process the picture information are entrusted. This infers the message inserting tasks must be directed completely finished the encoded area. What's more, like the instance of distributed computing, it is for all intents and purposes exorbitant to execute a dependable key administration framework (KMS) in such a multiparty domain over shaky open systems, because of the distinctions in possession and control of basic foundations on which the KMS and the secured assets are found.

1.3 State of Art Development

Since the first cover picture must be recouped in the wake of separating the mystery message, this prerequisite forced on reversible information concealing procedure a punishment of lower payloads, bigger contortion and higher computational cost-in contrast with those non-reversible strategies. In spite of these downsides,; recommending the expanding needs in this field. The reversible information concealing strategy created at the beginning time chiefly depends on lossless pressure procedure. In 2002, Fridrichet al. proposed a R– S conspire for which packed message bits were reversibly inserted in the status of gathering of pixels. Gelik et al. contrived a summed up slightest critical

bit(G-LSB) method to expand the payload of Fridrich et al. method. Awrangeb and Kankanhalli proposed a reversible plan that installed packed information into the first picture with the thought of the human visual framework to limit the detectable ancient rarities (Awrangeb et al., 2005). The strategies specified above included methodologies that inserted loss lessly packed highlights removed from the first cover picture. The other sort of reversible information concealing strategies can be ordered as expansion–installing based procedures. A typical element of these procedures is utilizing a stylistic theme connection administrator to make highlights with little sees. Information can be implanted by extending these highlights to make empty space into which message bits are installed.

The primary approach under this classification was proposed by (Tian, 2003), and stretched out by numerous ongoing investigates (Altar, 2004; Kamstra and Heimans, 2005; Thodi and Rodrigue, 2007; Kim et al., 2008). Extension inserting based methodologies for the most part experience the ill effects of unfortunate contortion when the estimations of highlights are expansive. In this manner, this strategy may notbe appropriate for applications where higher picture quality is de-manded. Another classification of reversible information covering up can be delegated histogram-moving based strategies. In these systems, a histogram of highlight components is made, and information can be inserted by moving histogram canisters. The outstanding method professional postured by Ni et al. in 2006 is of this class. Some other strategies can be found in H wang et al. and Fallahpour and Sedaaghi (2007). Shockingly, the limit of histogram-moving based systems is low and very reliant on the histogram dispersion of the cover picture. As a rule, the higher the pinnacle of picture histogram, the more the implanting limit is. Notwithstanding the procedures specified above, Coltuc acuainted an altogether different approach with reversibly implanted information in view of basic changes with low numerical many-sided quality.

These rising momentous reversible methods proposed the expanding consideration of getting. Numerous applications reuest brilliant pictures, for example, medicinal or military pictures. The outstanding reversible information concealing strategy proposed by Ni et al. can create moderately fantastic steno picture be that as it may, the inserting limit is low and is constrained by the appropriation of picture histogram. A few examinations depended on Ni et all's. strategy and were either attempting to improve the picture quality further or to build the installing limit. For instance, Xuan et al. proposed a novel ideal histogram match based reversible information concealing strategy utilizing whole number wavelet change and versatile histogram adustment with astounding execution. Nonetheless, their strategy included whole number wavelet changes (IWT) and ideal parameters choice, the computational cost is higher than Ni et al. strategy.

1.4 Watermarking

A watermark can be clarified as data that is inserted into information for discovery of alter, demonstrating proprietorship and so forth. It is utilized to check personality of the proprietor and in this manner make a copyright for the document. There are two stages in watermarking strategy called as watermarking inserting and extraction framework. Watermarking can be mostly grouped into two sorts unmistakable watermarking and undetectable watermarking. Obvious watermarking alludes to data noticeable on the document. They are installed logo mostly. For instance in an online magazine, the logo of the magazine is seen at an end. Undetectable watermarking influences data to install as a computerized information. It is for the most part utilized all around and can be recovered effectively.

1.5 Steganography

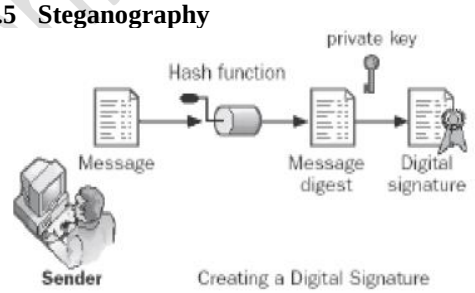


Fig .3 Steganography Block Diagram

Cryptography is the training and learning of procedures for secure correspondence within the sight of outsiders.

For the most part partitioned into two:-

- Public key cryptography (awry cryptography)Symmetric cryptography.

Open key cryptography requires two unmistakable keys-one of which is mystery and other is open.

- Symmetric cryptography depends on a similar key to perform both.

II.LITERATURE SURVEY

Tian, "Reversible data embedding using a difference expansion"Among the lossless methods of information installing there are two basic spaces of activity: spatial and recurrence. Spatial systems are portrayed by the implanting of messages into the minimum huge bits (LSBs) of picture pixels, while in recurrence strategies the message is installed after a

specific change is performed by altering recurrence coefficients of the cover picture.

As of late, the exploration on flag handling over encoded area has increased expanding consideration, principally determined by the requirements from distributed computing stages and different security saving applications. This has set off the examination of installing extra information in the scrambled pictures in a reversible design. In numerous down to earth situations, e.g., secure remote detecting and distributed computing, the gatherings that process the picture information are entrusted.

This infers the message inserting tasks must be directed completely finished the encoded area. What's more, like the instance of distributed computing, it is for all intents and purposes exorbitant to execute a dependable key administration framework (KMS) in such a multiparty domain over shaky open systems, because of the distinctions in possession and control of basic foundations on which the KMS and the secured assets are found.

2.1 EXISTNIG METHOD

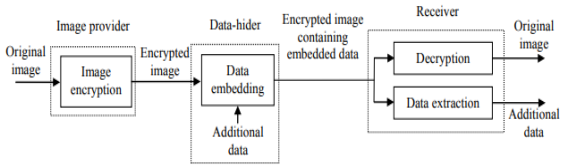


Figure 4 Sketch of lossless data hiding scheme for public-key-encrypted images

2.1.1 Image encryption

In this stage, the picture supplier scrambles a plaintext picture utilizing general society key of probabilistic cryptosystem pk. For every pixel esteem m(I,) where (I,) demonstrates the pixel position, the picture supplier ascertains its cipher text esteem,

c(I) E[p m(I) r(I)] k , = , (1)

where E is the encryption activity and r(I,) is an arbitrary esteem. At that point, the picture supplier gathers the cipher text estimations of all pixels to shape a scrambled picture. As a matter of fact, the proposed plot is capital with different probabilistic open key cryptosystems, for example, Parlier [18] and Damgard-urik cryptosystems [25]. With Parlier cryptosystem [18], for two expansive primes p and , compute n = p·, λ = lcm (p−1, −1), where lcm implies the slightest normal numerous. Here, it should meet that god (n, (p−1)·(−1)) = 1, where god implies the best regular divisor. The general population key is made out of n and a haphaardly chose number g in 2 * n , while the private key is made out of λ.

As a speculation of Parlier cryptosystem, Damgard-urik cryptosystem [25] can be additionally used to encode the plaintext picture. Here, people in general key is made out of n and a component g in 1 * s+ n with the end goal that g = (1+n) ·x mod ns+1 for a known moderately prime to n and x has a place with a gathering isomorphic to * n, and we may pick d as the private key when meeting d mod n ∈ * n and d = 0 mod λ. where r(I,) is an arbitrary number in 1 * s+ n . By applying a recursive adaptation of Parlier decoding, the plaintext esteem can be acquired from the cipher text esteem utilizing the private key. Note that, in light of the probabilistic property of the two cryptosystems, a similar dim qualities at various positions may relate to various cipher text esteems.

2.1.2. Information implanting

For each encoded pixel, the information hider chooses an arbitrary whole number r'(I,) in * n and figures. By survey the k-the LSB of scrambled pixels as a wet paper channel components of the wet paper channel, the information hider may utilize the wet paper coding [26] to implant the extra information by supplanting a piece of c(I,) with c'(I,). The points of interest will be given in the accompanying. Considering the principal LSB, if c(I,) are supplanted with c'(I,), the primary LSB in S1 would be flipped and the rest first LSB would be unaltered. Along these lines, the main LSB of the scrambled pixels can be viewed as a WPC, which incorporates alterable (dry) components and unchangeable (wet) components. At the end of the day, the primary LSB in S1 are dry components and the rest first LSB are wet positions.

By utilizing the wet paper coding [26], one can speak to by and large Ned bits by us flipping a piece of dry components where Ned is the quantity of dry components. In this situation, the information hider may flip the dry components by supplanting c(I,) with c'(I,). Meaning the quantity of pixels in the picture as N, the information hider may install by and large N/2 bits in the principal LSB-layer utilizing wet paper coding. Considering the second LSB (SLSB) layer, we call the SLSB in S2 as dry components and the rest SLSB as wet components. Note that the principal LSB of cipher text pixels in S1 have been controlled by supplanting c(I,) with c'(I,) or keeping c(I,) unaltered in the main LSB-layer installing, implying that the SLSB in S1 are unchangeable in the second layer. At that point, the information hider may flip a piece of SLSB in S2 by supplanting c(I,) with c'(I,) to insert all things considered N/4 bits utilizing wet paper coding. So also, in the k-the LSB layer, the information hider may flip a piece of k-the LSB in Ski to insert all things considered N/2k bits. At the point when the information implanting is actualized in K layers, the aggregate N·(1−1/2K) bits, by and large, are installed. That suggests the implanting rate, a proportion between the quantity of inserted bits and the quantity of pixels in cover picture, is around

(1−1/2K). That suggests the upper bound of the implanting rate is 1 bit for every pixel. The following subsection will demonstrate that, in spite of the fact that a piece of c(I,) is supplanted with c'(I,), the first plaintext picture can at present be acquired by unscrambling.

2.1.3. Information extraction and picture decoding

After getting a scrambled picture containing the extra information, if the beneficiary knows the information concealing key, he may figure the k-the LSB of encoded pixels, and afterward extricate the installed information from the K LSB-layers utilizing wet paper coding. Then again, if the collector knows the private key of the utilized cryptosystem, he may perform unscrambling to acquire the first plaintext picture. At the point when Parlier cryptosystem is utilized, The decoding on c'(I,) will likewise result in the plaintext esteem.

2.1.4 RIDH SCHEME OVER ENCRYPTED DOMAIN

Rather than considering committed encryption calculations custom fitted to the situation of scrambled space information concealing, we here adhere to the customary stream figure connected in the standard organization. That is, the figure content is created by bitwise Coring the plaintext with the key stream. If not generally determined, the broadly utilized stream figure AES in the CTR mode (AES-CTR) is accepted.

Flowchart of the proposed work is given beneath,

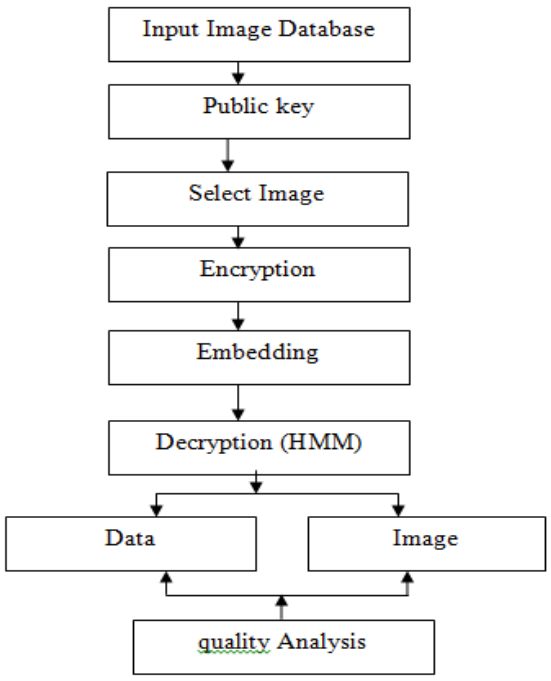


Fig 5. Flow Chart Of Proposed System

The subsequent information concealing worldview over scrambled space could be all the more for all intents and purposes valuable in view of two reasons.

- Stream figure utilized in the standard organization (e.g., AES-CTR) is as yet a standout amongst the most prominent and dependable encryption instruments, because of its provable security and high programming/equipment usage productivity. It may not be simple, or even infeasible, to induce clients to embrace new encryption calculations that have not been altogether assessed.
- Large measures of information have us been encoded utilizing stream figure standard. At the point when stream figure is utilized, the scrambled picture is produced by

[[f]]=Enc(fake)=fake (1) where f and [[f]] signify the first and the scrambled pictures, individually. Here, K signifies the key stream produced utilizing the mystery encryption key K . In this paper, without loss of sweeping statement, every one of the pictures is thought to be 8 bits. All through this paper, we utilize [[x]] to speak to the scrambled rendition of x. Unmistakably, the first picture can be gotten by playing out the accompanying unscrambling capacity:

f=Dec([[f]],K)=[[f]]⊕K. (2)

As said before, the scrambled picture [[f]] now fills in as the cover to suit message to be covered up. We first gap [[f]] into a progression of non covering obstructs [[f]]if's of see M × N, where I is the square file. Each square is intended to convey n bits of message. Giving the quantity of squares inside the picture a chance to be B, the inserting limit of our proposed conspire moves toward becoming n • B bits. To empower effective implanting, we propose to utilize S = 2n parallel open keys 0, 1,..., S−1, every one of which is of length L = M × N × 8 bits. All 's, for 0 ≤ S − 1, are made openly available, which suggests that even the aggressor knows them. These open keys are preselected preceding the message installing, as per a model of augmenting the base Hamming separation among all keys. The calculation created by MacDonald can be utilized to this end.

III.PROPOSED SCHEME

This section explains the proposed watermarking mechanism in detail. In order to satisfy image authentication and copyright protection requirements, a blind invisible dual watermarking mechanism for color images is presented. The details

of dual watermark embedding and extraction phases of our proposed mechanism are described in Sections III-A and III-B, respectively

- Dual Watermark Embedding Fig. 1 shows our watermark embedding procedure. The process of embedding the watermark is divided into two phases: 1) embedding the invisible robust watermark and 2) embedding the invisible fragile watermark.
- Phase 1 (Embedding the Invisible Robust Watermark) Initially, the original RGB color image is converted into YCbCr color space. The basic equations used to convert RGB

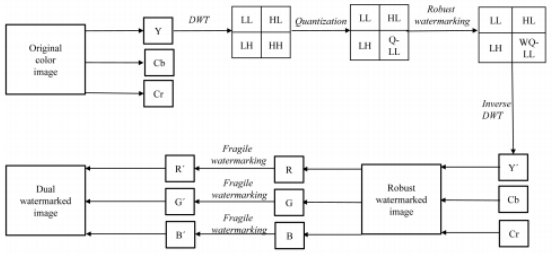


Fig 6. Our watermark embedding procedure

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Fig 7. Luminance quantization table [11].

into YCbCr are Y = 0.299R + 0.587G + 0.114B Cb = −0.172R − 0.339G + 0.511B + 128 Cr = 0.511R − 0.428G − 0.083B + 128. (1)

After YCbCr conversion, the one-level DWT decomposition of Y is performed to generate the LL, low–high (LH), high–low (HL), and HH sub-bands, where LL consists of the approximation part of the original Y channel, and the remaining three resolution sub-bands consist of the detailed parts, which are very difficult for the human eye to discern. Thus, we used this characteristic for our robust watermarking scheme. First, the LL sub-band is divided into several 8 × 8- sized blocks, and then, each pixels of a block is quantized by directly dividing it by the corresponding value of the luminance quantization table [30], as shown in Fig. 2. After all of the blocks have been quantized, a quantized LL (QLL) sub-band is generated, and the HH sub-band is directly replaced by the resulting Q-LL sub-band. This is because the Q-LL sub-band would hardly be changed while suffering malicious attacks. This characteristic allows the blind and robust decoding during watermark extraction procedure. After that, the robust watermark is embedded in the Q-LL sub-band to produce a watermarked Q-LL (WQ-LL) sub-band with WQLLn = QLLn + WRn ∗ k (2) where QLLn is the pixel value in the Q-LL sub-band, WQLLn is the resulting pixel value in the WQ-LL sub-band, WRn is the embedded robust watermark bit, and k is a constant parameter that corresponds to the strength of the watermark. A higher k can increase the strength of the embedded watermark, but it makes the watermarked image easier to perceive.

After embedding the watermark, the inverse DWTs of the four resulting sub-bands, i.e., LL, HL, LH, and WQ-LL, are performed to generate the watermarked Y channel. Then, the watermarked Y , Cb, and Cr channels are converted back into RGB and saved as the robust watermarked image. Phase 2 (Embedding the Invisible Fragile Watermark)

The robust watermarked color image is generated after robust watermarking. In this phase, the same fragile watermark (WF) for image authentication is embedded independently on each RGB color channel of the robust watermarked image. For each channel, i.e., R or G or B, first, we transform the fragile watermark bitstream WF into a sequence of digits W F using a 3n-base notational system, where n is a parameter. Later, each digit in sequence W F is treated as one hidden digit s, which can be embedded into an n-pixel unit U = (p1, p2,..., pn) of each channel. The basic idea of the embedding procedure is to perform the LSB replacement for unit U in 3n-base notational system. The detailed embedding process of each hidden digit s is described in detail as follows.

Step 1: A digit E is extracted from each n-pixel unit U using (3). Here, function

() is defined as an extracting function that is also used for extracting the fragile watermark in Section III-B. This equation is equivalent to extract the LSB of unit U in 3n-base notational system, and pi can be regarded as a digit in unit U E = I(p1, p2,..., pn) = n i=1 3i−1 pi mod 3n. (3)

Step 2: To embed hidden digit s, the digits in unit U need to be adjusted and make sure that the resulted E equals s. Therefore, a temporary value t is generated for adjusting the original unit U using t = s − E +

3n − 1 2 mod 3n. (4)

Step 3: To match each digit pi in unit U, the temporary value t is transformed into a sequence t using a 3-base notational system, where t = b1b2 ... bn, bi is a digit in t and 1 ≤ i ≤ n.

Step 4: Based on the ternary modulation property, each digit in sequence t is then reduced by 1 to generate a subtracted sequence t = d1d2 ... dn, where di = bi − 1. \

Step 5: Each pixel of the original n-pixel unit U is added to a corresponding digit of subtracted sequence t using (5) to generate the watermarked pixel unit U = (p 1, p 2,..., p n). Therefore, the extracted E from unit U would be identical to hidden digit s p i = pi + d j, where 1≤ i ≤ n and j = n − i + 1. (5)

These steps are repeated until all of the digits in sequence W F are embedded in each RGB color channel of the robust watermarked image, resulting in a dual watermarked Fig. 3. Example of embedding a fragile watermark. image. To make it easier to understand, an example of the fragile watermarking procedure is illustrated as follows. Assume that the left table in Fig. 3 is a 4 × 4-pixel block of the R channel, watermark WF is (111111)2, and n is set as 2. First, WF = (111111)2 is transformed into W F = (70)9 using a 32-base notational system. Therefore, there are two hidden digits in W F = (70)9, one of which is 7 and the other is 0. We choose pixels 44 and 45 as the 2-pixel unit U = (44, 45) to embed hidden digit s = 7. Using (3), digit E = 8 is extracted from U. Later, using (4), the temporary value t = 3 is calculated, and it is transformed into a sequence t = (10)3 using a 3-base notational system.

Then, each digit in sequence t is reduced by 1 to generate a reduced sequence t = (0, −1). The watermarked pixel unit U = (43, 45) can be obtained using (5), i.e., p 1 = p1 + d2 = 44 − 1 = 43, p 2 = p2+d1 = 45+0 = 45. In a similar way, unit (37, 31) can be generated as a watermarked unit (36, 30) while embedding the other hidden digit 0. Therefore, after embedding watermark WF = (111111)2, a new 4 × 4-pixel block of the R channel is generated, as shown in the right table in Fig. 3. As a special case, underflow or overflow would occur when the watermarked pixel p i is less than 0 or greater than 255, respectively. To solve with either an underflow or overflow situation, the original pixel pi , which would result in underflowed or overflowed p i , is increased by 1 or reduced by 1, respectively. After that, the proposed embedding algorithm is repeated to generate a new pixel unit U . This procedure is repeated until all pixels in the new pixel unit U range between 0 and 255.

D. Extraction of the Dual Watermark

In the proposed extraction procedure, the robust watermark and the fragile watermark can be extracted separately for the purpose of copyright detection and image authentication, respectively. The two different usages are described in detail in the following. In terms of copyright protection, the process of extracting the robust watermark begins with converting the watermarked RGB image into YCbCr color space. After the YCbCr conversion, the one-level DWT decomposition of Y is performed to generate the LL, LH, HL, and HH sub-bands. Then, the LL sub-band is divided into several 8 × 8-sized blocks, and each pixel of the block of host image is quantized by directly dividing it by the corresponding value of the luminance quantization table, as shown in Fig. 2. After all of the blocks are quantized, a Q-LL sub-band is generated.

Then, the robust watermark is extracted by WRn = (HHn − QLLn)/k (6) where QLLn is the pixel value in Q-LL sub-band, HHn is the corresponding pixel value in HH sub-band, WRn is the extract robust watermark bit, and k is a constant parameter that is the same as that in the watermark embedding procedure. After all of the robust watermark bits have been extracted from the watermarked image, the owner of this image can be identified. Note that the extraction of the robust watermark is blind in that it does not require the original image or any information regarding the watermark. Concerning image authentication, the extraction of the fragile watermark is proceeded by extracting three completed watermark bitstreams in the R, G, and B channels of the watermarked image separately. For each n-pixel unit in each channel, a hidden digit can be extracted using the extracting function, as shown in (3). After extracting all of the hidden digits, the hidden sequence is transformed using a 2-base notational system to provide an extracted watermark bitstream of each channel. The three extracted watermark bitstreams are compared with the original fragile watermark, and if the watermark bit of any one of the extracted watermark bitstreams is not the same as the original watermark bit, the corresponding pixel is regarded as being modified, and we mark it with a dark color. Therefore, the integrity of the image can be detected, and the tampered area can be located accurately.

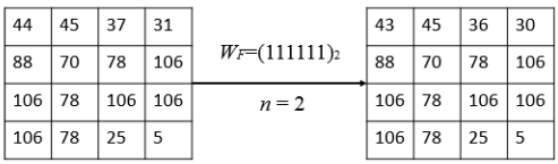
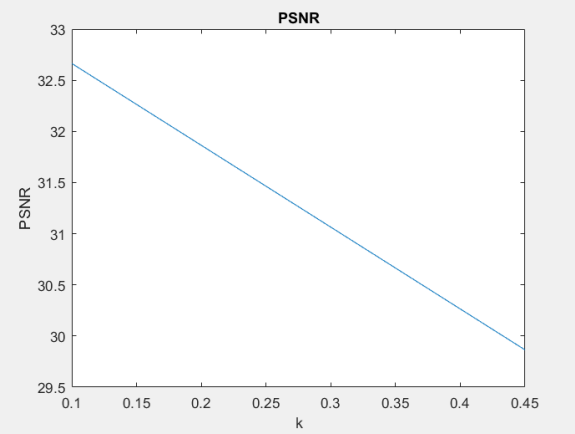


Fig 8. Example of embedding a fragile watermark

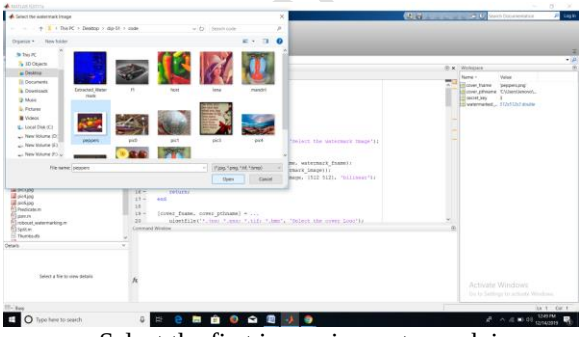
IV. RESULT ANALYSIS
EXISTENCE METHOD

In this existance method initially we select the watermark image and we select coverimage .By these two images robust watermarking is performed and finally we get output as watermarked image in extraction method.

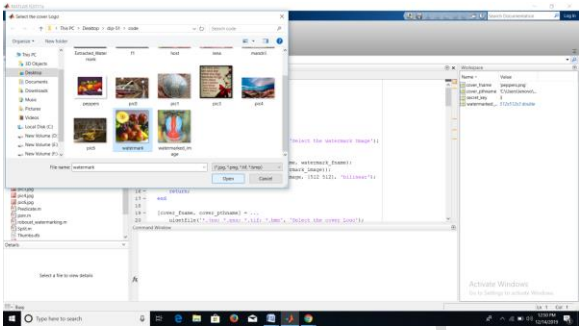


The above figure represents the PSNR graph values. By using this graph we can calculate the PSNR values.

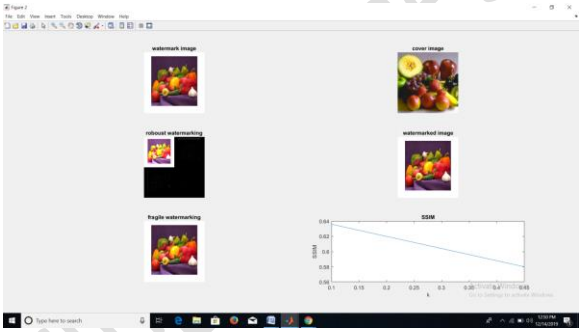
PRORPOSED METHOD RESULT



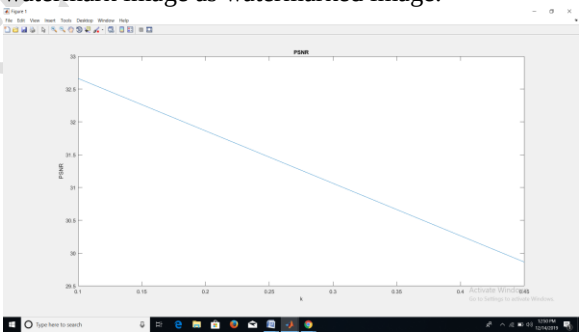
Select the first image i.e.,watermark image as peppers



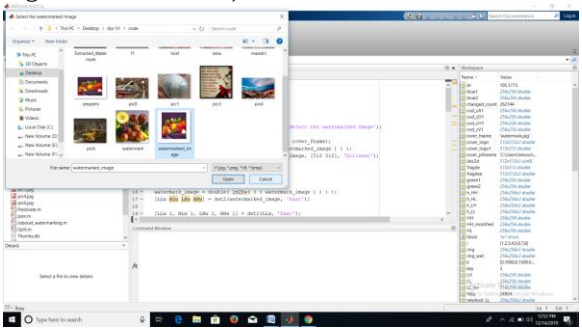
The second image we select is cover image as watermark



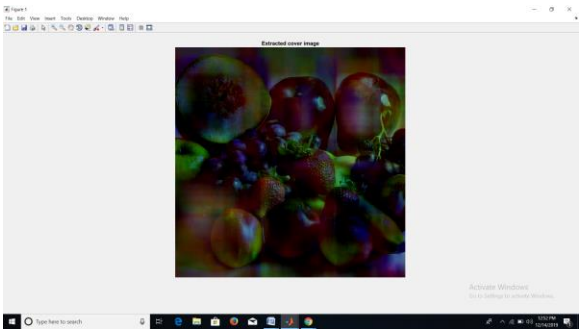
The output is generated as above where the fragile watermarking is done here and we get watermark image as watermarked image.



The above figure represents PSNR(Peak Signal to Noise Ratio) values table.



Now select the watermarked_image to extract the cover image.



When we select the watermarked image, the watermark_extraction method generates the Extracted cover image.

Advantages

- Low complexity and easy implementation
- More robustness
- Not affect the visual quality of the image
- Improves the picture quality

Applications

- Security based applications
- Validity protection

V.CONCLUSION

In this paper, we presented a blind dual watermarking mechanism for color the authentication of images and copyright protection. The invisible, fragile, and robust watermarks are embedded into the spatial domain of the RGB color space and into the frequency domain of the YCbCr color space. The major contribution of this paper is that our mechanism can achieve copyright protection and image authentication simultaneously, and the extraction of watermarks from the protected image can be processed blindly without the original host image and watermarks. According to the experimental results, the proposed watermarking mechanism can withstand various processing attacks and locate the tampered area of the image accurately. Moreover, the dual watermarked image is imperceptible, which makes the proposed mechanism suitable for protecting valuable original images. Comparisons of the functionality of our proposed mechanism with the functionalities of other well-known dual watermarking mechanisms clearly demonstrated the superiority of the proposed mechanism.

VI. FUTURE SCOPE

As a future work, we plan to extend the proposed approach to video watermarking domain. As the embedding and the extracting processes are of low complexity and do not require any specific features of the input image, the extension to video watermarking will be straightforward. Along with that, an automatic technique for the selection of the gain factor value needs to be developed to have better control on both imperceptibility and robustness of the scheme**.**

REFERENCES

[1] M. U. Celik, G. Sharma, A. M. Tikal, and E. Saber, "Lossless summed up LSB information inserting," IEEE Trans. Picture Process., vol. 14, no. 2, pp. 253– 266, Feb. 2005.

[2] M. U. Celik, G. Sharma, and A. M. Tikal, "Lossless watermarking for picture verification: another system and a usage," IEEE Trans. Picture Process., vol. 15, no. 4, pp. 1042– 1049, Apr. 2006.

[3] . Ni, Y.- . Shi, N. An sari, and W. Su, "Reversible information concealing," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354– 362, Mar. 2006.

[4] X. Li, W. hang, X. Guy, and B. Yang, "A novel reversible information concealing plan in view of two-dimensional contrast histogram adustment," IEEE Trans. Inf. Criminology Security, vol. 8, no. 7, pp. 1091– 1100, up. 2013.

[5] C. in, C.- Caching, Y.- H.Huang, and L.- T. Liao, "An inpaintingassisted reversible Steganography conspire utilizing a histogram moving component," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109– 1118, up. 2013.

[6] W.- L. Tai, C.- M.Yeh, and C.- C. Chang, "Reversible information stowing away in view of histogram adustment of pixel contrasts," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906– 910, un. 2009.

[7] . Tian, "Reversible information implanting utilizing a distinction extension," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890– 896, Aug. 2003.

[8] Y. Hu, H.- K. Lee, and . Li, "DE-based reversible information covering up with enhanced flood area outline," Trans. Circuits Syst. Video Technol., vol. 19, no. 2, pp. 250– 260, Feb. 2009. [9] X. Li, B. Yang, and T. eng, "Effective reversible watermarking in view of versatile expectation blunder extension and pixel determination," IEEE Trans. Picture Process., vol. 20, no. 12, pp. 3524– 3533, Dec. 2011.

[10] X. hang, "Reversible information stowing away with ideal esteem exchange," IEEE Trans. Mixed media, vol. 15, no. 2, pp. 316– 325, Feb. 2013.

[11] T. Bianchi, A. Piva, and M. Barni, "On the execution of the discrete Fourier change in the encoded space," IEEE Trans. Inf. Criminology Security, vol. 4, no. 1, pp. 86– 97, Mar. 2009.

[12] T. Bianchi, A. Piva, and M. Barni, "Composite flag portrayal for uick and capacity effective preparing of scrambled signs," IEEE Trans. Inf. Criminology Security, vol. 5, no. 1, pp. 180– 187, Mar. 2010.