Abstract—In various applications, images are sensitive and prone to attacks such that any modification in it could lead to serious problems. For example, altering any region of a medical image could lead to wrong treatments. Thus, detecting forgery / counterfeit in images are a mandatory and recovery of tempered regions is necessary.

The main share of this paper is to propose a new Dual Watermarking (DW) scheme, which aims at detecting any modification, forgery / counterfeit, or illegal manipulation of images even if it is tiny. Our proposed scheme is a secure, fragile, and a reversible watermarking scheme. This scheme dynamically generates the watermark using messy models. A Chaotic model is iteratively applied to produce the chaotic sequences based on the initial values, which are determined by combining the values of pixels of image, position information and key.

It is embedded inside the image by expanding intra plane difference between any two color planes of image. It is known as intra-plane difference expanding. At the receiver, a detector extracts the watermark and localizes the tampered regions without access to the host image or the original watermark. The tempered regions are recovered using alpha channel embedded in image, thus recovered image is a grayscale image. The proposed scheme is very sensitive to modifications anywhere in the image even if it is too small.

Keywords—chaotic system, digital Image, Image authentication, integer transform, reversible, fragile.

I. INTRODUCTION

Development of the Internet and digital multimedia provides us great advantages such as high quality lossless digital media, easy editing, and high fidelity copying. This ease, by which digital information can be manipulated and duplicated, has made publishers, authors, medical images, artists, and photographers afraid that their innovations and products going to be modified illegally or claimed by others. Therefore, we need a technique for verifying content’s integrity of the digital media and recover tempered regions. Copyright protection and Authentication plays an important role here. Copy right protection protects owner's intellectual property and traces the illegal copies of the content. Authentication checks that the received image has been altered or not and localize the tampered regions. In general, watermarking techniques used for integrity authentication have the following properties [1] [2].

1) Tamper detection: This is the fundamental feature to a tamper proofing system, in this detector in the system should determine whether an image is veritable.
2) Localization of modification: The verification result after extraction should be able to reflect and locate the modified regions.
3) Perceptual transparency: An embedded watermark should be perceptually invisible under normal observation.
4) Blind detection: The authentication process of Image does not require host image. Image is verified using embedded watermark.
5) Robust or fragile property: Most fragile and semi-fragile algorithms aim to detect the malicious tamper operations. However, robust schemes can also serve this purpose.

In Messy Watermarking [1] the system dynamically generate the watermark using messy system which is unique for every image. The generated watermark is then embedded in the original image by expanding the differences of the pixel pair formed in intra color planes of the images. Messy system is a dynamical system whose behavior changes with time.

Fragility [1] refers that the digital image should be sensitive to various attacks. Therefore, the watermark should be easily broken in order to authenticate the digital images. It has been observed that if lower size of the watermark could sense the modification, thereby some of the watermark bits are changed; then, the higher size of the watermark will also sense the modification. For the other sizes, it is linearly increased. This test results are average of various level of modification results for jittering attack. It is a common attack in any kind of watermarking scheme.

Dual Watermarking [8] Scheme based on DWT with chaos encryption algorithm, will be developed to improve the robustness and protection along with security. Two watermarks are embedded in the host image. The secondary is embedded into primary watermark. This provides an efficient and secure way for image transmission. The reliable watermark extraction scheme is developed for the extraction of the primary as well as secondary watermark from the distorted image.
Reversible watermarking [6] algorithm with very high data hiding capacity has been developed for color images. The algorithm allows the watermarking process to be reversed, which restores the exact original image. The algorithm hides several bits in the difference expansion of vectors of adjacent pixels. The required general reversible integer transform and the necessary conditions to avoid underflow and overflow are derived for any vector of arbitrary length. In many applications, images are sensitive to an extent such that any modification in it could lead to serious problems, which aims at detecting any modification, forgery, or illegal manipulation of images even if it is small. Extracted watermark must be compared with generated watermark from received image, if there are any divergence in watermark, then image is tempered.

II. PROPOSED WATERMARKING SCHEME

The proposed watermarking scheme consists of dual watermarking [8] scheme for better security of the image and recovery, it works in five stages. The first stage selects the reference color plane for generating watermark. The second stage generates the watermark using the reference color plane through messy system [1]. The embedding process is carried out using integer transform in the third stage. Alpha channel [8] [9] is generated and 32 bit TGA image [8] is formed in fourth stage i.e. Dual Watermark. The fifth stage performs the extraction and verification process. If image is tempered then it is recovered through the alpha channel which gives gray scale image.

A. Identification of Reference Color Plane

In this phase, we use digital image as input to the system. Then we split the given digital image into its three bit planes. Since, each pixel of the image is of 24-bit, we divide it into 3 different bytes of RGB planes. Then we select a reference plane whose least significant bit of every pixel in the digital image would be used to generate the watermark that is needed during embedding phase. That is we store the least significant bit values for every pixel for a reference plane and use it for producing watermark. As every image might have different least significant bit values it would help us producing the watermark in dynamic way. We will not be considering the reference plane for pixel difference expansion the other two planes will be considered for pixel difference expansion.

The pixels of digital image in the proposed scheme are given in 24-bits. The green channel of the digital image contains the important details than other color channels. Hence, the green color plane is chosen as reference color plane to generate the watermark.

It can also be done according to the color characteristics for other imaging modalities such as CT Scans, X-Ray and MRI. We split the given image into the bit planes as shown in figure 1.

![Figure 1](image.png)

**Figure 1** A) Original Image  B) Green Plane C) Blue Plane D) Red Plane Separation of RGB Planes

B. Generating Watermark Using Messy System

Messy system [1] is a dynamic system whose behavior changes according to time. These changes are very sensitive to the initial conditions. Thus, the behavior of messy system appears to be random, though they are deterministic. The dynamic changes of this system are completely defined by their initial conditions without any random elements. Therefore, the watermark is generated through messy system using the reference color plane as initial condition. Thereby, the watermark is generated dynamically. A general messy system is defined by the following equation [1] [2] [3].

\[ X_{n+1} = f(X_n) \] (1)

Where \( f(\cdot) \) refers the iterative, nonlinear function. It iteratively produces the values for initial value. It is known as messy sequence.

In the proposed system, a hybrid optical bi stable messy system [2] is used which is defined by

\[ f(X_n) = 4sin^2(X_n - 2.5) \] (2)

The watermark is generated through messy system by using prominent pixel values of reference color plane of the image as seed pixel. The initial values to the messy system is designed by

\[ x_{seq}(k,0) = a*floor(s(k)/2^3) + b*pos + c*key \] (3)
Where, s(k) refers the pixel values of reference color plane of the image. \( a, b, \) and \( c \) are predefined constants and \( l \) refers embedding depth. The position information (pos) and secret key (key) is also used in the initial condition. The messy sequence is generated by substituting \( x_{\text{seq}}(k,0) \) value for \( X_n \) in Eqn.2. For the \( k \)th pixel the sequence is referred as \( x_{\text{seq}}(k, i), i=1, 2, 3 ... l \). The reasonable number of iteration (I) is performed for the \( k \)th pixel to attain the messy status e.g. If image is of size 512 X 512, then there will be 512*512 possible iterations.

The watermark generated is dynamic and is unique for every image chosen for watermarking. In this phase, we encrypt the watermark with the help of some external key. This same key is required to extract the watermark at verification phase.

This sequence contains floating numbers that is converted into binary sequence in the proposed scheme. Hence, the thresholding \( T \) is introduced here to convert the sequence \( x_{\text{seq}}(k, i) \) from floating to binary sequence \( w(k,i) \) obtained by

\[
w(k,i) = \begin{cases} 
1 & x_{\text{seq}}(k, i) > T \\
0 & \text{Elsewhere} 
\end{cases}
\]

(4)

Where, threshold value \( T \) is set to 8/3 by the number of test to bring equal number of zeros and ones.

By repeating the same procedure for remaining pixels of the reference color plane of the image, the watermark is generated for the whole image.

C. Embedding By Intra Plane Difference Expanding

The watermark generated in preceding stage will be embedded in this stage by using intra-plane difference expanding. In the embedding stage, the original image \( Image \) \((P, Q, R)\) is divided into color planes. Here \( P \) denotes number of rows, \( Q \) denotes number of columns and \( R \) denotes number of planes. \( k=3 \) as image is in RGB mode. The one color plane will be used as seed to generate the watermark in messy system. Since, the watermark is generated dynamically; it will be unique to the images.

Then, pixel pair is formed from the red and blue color planes of the images. By checking overflow and underflow condition for pixel pair, the watermark is embedded in the difference of the pixel pair by expanding the difference. This is known as intra-plane difference expanding \([1-6]\).

**Integer Transform:** For a 8 bit gray scale pixel pair \((x, y), 0 < (x,y) < 255\), the integer transform is given by the pair \((m, d)\). Where \( m \) refers integer average and \( d \) refers difference.

\[
m = (x + y)/2 \quad (5)
\]

\[
d = (x - y) \quad (6)
\]

---

**Figure 2:** Watermark Generation Process

**Figure 3:** A) Original Image  
B) Watermark Generated from Green Plane

**Figure 4:** Embedding Process
Inverse Transform is given by

\[ x = m + (d+1) / 2 \]  \hspace{1cm} (7)

\[ y = m - (d / 2) \]  \hspace{1cm} (8)

In the integer transform, the difference \( d \) is modified based on the watermark bit (bit) to hide the bit into the pixel pair. The modification of difference \( d' \) is given by

\[ d' = 2 * d + \text{bit} \]  \hspace{1cm} (9)

The modification process checks two conditions. They are overflow and underflow. It is done to ensure that the difference is expandable or not. The expandable difference should satisfy the following condition.

\[ d' \leq 2 * (255 - m) \]  \hspace{1cm} if \( 128 \leq m \leq 255 \)  \hspace{1cm} (10)

\[ d' \leq 2 * m + 1 \]  \hspace{1cm} if \( 0 \leq m \leq 127 \)  \hspace{1cm} (11)

In the proposed scheme, the pixel pairs are formed from red and blue color plane's pixel values. This is known as intra plane difference expanding. Thus, the difference between the pixels from different (Red and Blue) color planes is expanded for embedding watermark in the proposed scheme. Thereby, the watermarked image (W_img) is generated for the given Original image (Img).

**D. Generation Of Second Watermark Using (α-Channel)**

After embedding the first dynamically generated watermark with the help of pixel difference expansion in the image, the watermarked image (W_img) in this phase is again split into RGB planes. We here use the concept of the α-channel. [8] [9] This watermark is again dynamic and is unique, as it is generated from the pixels of the image again. Here, what we do is, we generate α-channel with the help of the red, green and blue values of all pixels. The average of the RGB values for every pixel in the image is found out for the generation of the α-channel. The α-channel consists of average of RGB values for all the pixels of the image. This α-channel acts as verification information to find out if the image has been tampered or not. The α-channel value is given by following equation

\[ \alpha = (R+G+B)/3 \]  \hspace{1cm} (12)

It is calculated for all pixels in the image in order to produce the α-channel

**Embedding Of α–Channel**

In this phase the α-channel generated within the last phase is embedded within the watermarked image (W_img), along with the undisturbed red, green and blue pixels of the every plane of the image. In this phase 32-bit TGA image [8] [9] is generated from watermarked image (W_img). In which first 24 bit stores the RGB planes of watermarked image (W_img) and next 8-bit will store the α-channel values.

This watermark is again unique and dynamic for the image. The values of the pixel are kept undisturbed in the image because the image should not be affected because of the watermark produced in the last phase. This phase produces the image with dual watermarking [8]. Now the dual watermarked image consists of both watermarks i.e. first watermark produced with the help of reference plane’s least significant bit values and the second watermark generated within the last phase.

**E. Extraction And Verification**

In the extraction process, the watermarked image W_img is processed in the same way as original image processed for embedding. The extraction process is complete blind. Both original image and original watermarks are not used for the extraction process.

In this phase we check if the image has been damaged or not with the help the two watermarks that we have embedded as proposed in the paper.
As the \( \alpha \)-channel is embedded second in the first phase of extraction we check the image has been damaged or not with the help of the \( \alpha \)-channel embedded. The average of the pixel values of the given image will be compared to \( \alpha \)-channel. If the average for pixel values has been damaged it would simply detect that the image has been damaged. We will be extracting the \( \alpha \)-channel and comparing it with the current average pixel values so as to find out the damaged pixels of the image.

If we cannot detect any changes with the help of \( \alpha \)-channel then we try to detect the changes with the help extracting the first watermark. Extraction process produces the reference sequence using messy system and green color plane as seed. The embedded watermark is extracted by applying inverse integer transform. Where, the LSB (Least Significant Bit) \[1\] \[2\] \[3\] of the difference value gives the embedded watermark bit. The reference sequence and the extracted watermark sequence are compared to check that whether the given volume of the image is tampered or not. The difference between reference sequence and the extracted watermark sequence will show the tampered regions in the image.

Thus, the extraction process works in complete blind way and enhances the security. The extraction process in this paper is reversible. It means that the original image should be retrieved without any loss after removing the watermark at the extraction stage. The medical images were exchanged from one place to another for diagnosis purposes. Hence, the loss in the quality of images is not accepted here.

**III. Conclusion**

The proposed method uses dual watermarking scheme for copyright protection of image and recovery of image. It generates both the watermarks dynamically. The watermarks generated are unique for every image. We are embedding the First watermark with the help of pixel difference expansion of other planes. The second watermark would be containing the average of the pixel values of image. If it is detected that image is tempered than it is recovered using alpha channel, but recovered image will be a grayscale image. The system would be able to produce better results than the systems proposed before as it uses dual watermarking and thus, help us to protect the image from its unauthorized use.

**REFERENCES**


