*Volume 10, Issue 1, January – 2025* *International Journal of Innovative Science and Research Technology (IJISRT)*
*ISSN No:-2456-2165* *https://doi.org/10.5281/zenodo.14724997*
*IJISRT25JAN635* *www.ijisrt.com*

# Multi-Channel Statistical Framework for Robust and Reliable Watermark Detection in Color Image Processing

Nafla Iqbal[1]

Assistant Professor
Department of Artificial Intelligence and Data Science Rajagiri School of Engineering and Technology
Kakkanad, India

Publication Date: 2025/01/24

**Abstract**

Information security has become a critical aspect of modern life. One viable approach to ensuring secure and legitimate transactions is by embedding data into multimedia content, such as through watermarking. This paper introduces a novel watermarking scheme for color images, along with its corresponding detector. Although numerous methods for watermark detection exist, the integration of Hidden Markov Models (HMMs) has significantly improved the accuracy of watermark extraction from color images. Unlike many existing systems that overlook inter-channel dependencies, this work emphasizes the role of inter-channel dependencies between RGB channels. Additionally, it leverages inter-scale dependencies of sparse coefficients for color images using HMMs, offering a more robust and accurate watermarking solution.

***Keywords*:** *Information Security, Watermarking, Hidden Markov Model, Inter-Channel Dependencies.*

## I. INTRODUCTION

Secure multimedia data transmission is a critical area of re- search, and embedding information within multimedia signals offers an effective approach to achieve this objective. Multi- media messages can be safely validated at the recipient's end by using encryption and decryption techniques.Watermarking is the process of adding a secret key to the original image to provide authentication and verify ownership.Color picture watermarking has gotten relatively little attention despite its increasing significance in contemporary multimedia applica- tions, but grayscale watermarking has seen major developments.

Utilizing the RGB channels' dependencies and correlations effectively is one of the challenges of watermarking color photos. Making good use of these inter-channel interactions can improve the watermarks' resilience and detection preci- sion. The importance of modeling RGB channel dependencies for successful watermark embedding and detection has been highlighted by earlier research, such as the watermarking approach shown in [5]. Another important technique, in [6], further explains the potential of inter channel correlations in enhancing the effectiveness of watermarking by modeling wavelet coefficients and their inter-channel dependencies using the multivariate power-exponential distribution.

Building upon these foundational insights, this work pro- poses a novel multiplicative multi-channel watermark detector specifically designed for color images. The proposed scheme utilizes Hidden Markov Models (HMMs) in the contourlet domain to capture and exploit both inter-channel and inter- scale dependencies. The contourlet transform offers supe- rior directional and multi-resolution representation capabilities compared to traditional wavelet transforms, making it an ideal choice for this application. By incorporating HMMs, the scheme achieves a more sophisticated statistical modeling of the dependencies, thereby improving detection robustness and accuracy.

To evaluate the effectiveness of the proposed scheme, ex- tensive experiments were conducted, testing the watermarked images under various distortion scenarios, including com- pression, filtering, and noise. These distortions were chosen to simulate real-world challenges that watermarked images may encounter. The results demonstrate that the proposed watermarking scheme provides a robust solution, maintaining detection performance even under adverse conditions.

Nafla Iqbal, (2025), Multi-Channel Statistical Framework for Robust and Reliable Watermark Detection in Color Image Processing. *International Journal of Innovative Science and Research Technology*, 10(1), 743-750. https://doi.org/10.5281/zenodo.14724997

Overall, this work contributes to advancing the field of color image watermarking by addressing the often-overlooked aspect of inter-channel dependencies and introducing a robust detection mechanism that leverages HMMs in the contourlet domain. This approach not only enhances the reliability of watermarking systems but also paves the way for further research in secure multimedia data transmission.

## II. LITERATURE SURVEY

### *A. A New Blind Wavelet Domain Watermark Detector using Hidden Markov Model*

This paper focuses on the development of a locally-optimum watermark detector utilizing a Hidden Markov Model (HMM) for modeling image wavelet coefficients. The approach is grounded in the observation that image wavelet coefficients exhibit heavy-tailed marginal statistics and exhibit strong inter- and intra-subband dependencies. To accurately capture these characteristics, the proposed method leverages a vector- based Hidden Markov Model (VHMM), an advanced statistical framework capable of effectively modeling the dependencies inherent in wavelet coefficients.

The wavelet transform, a cornerstone of modern signal processing, is particularly well-suited for watermarking appli- cations due to its unique properties. These include locality, multi-resolution analysis, and compression, which simplify signal processing tasks. In addition to these fundamental prop- erties, wavelet transforms exhibit distinctive characteristics such as non-Gaussianity, clustering, and persistence across scales, which further enhance their applicability to robust watermarking schemes.

Digital image watermarking, which involves the impercep- tible embedding of watermark bits into a host image, plays a crucial role in copyright protection and authentication. The process typically consists of two primary steps:

Embedding: The watermark is inserted into the host image. Detection: The presence of the watermark is verified when the image is received using a watermark detector. A critical requirement for wavelet-based watermarking is the design of a blind detector, which does not rely on the original image for verification.

The first step in watermarking is to apply a two-level wavelet transform to the host image. The image undergoes decomposition into subbands, each of which represents a distinct frequency component. Particular subbands contain the watermark bits, and statistical analysis is used to choose the target subband. To improve robustness and imperceptibility, the subband with the highest energy or other advantageous statistical characteristics is usually selected. In order to encode the watermark while maintaining the visual quality of the image, the embedding procedure alters the coefficients of the chosen subband.

Using the suggested HMM-based detector, the wavelet transform is applied to the possibly watermarked image, and the coefficients of the targeted subbands are examined. Utilizing the statistical model that VHMM offers, the detector reliably detects the watermark's existence despite distortions like compression, noise, or filtering.

To create a reliable watermarking technique, the suggested method makes use of wavelet coefficients' statistical character- istics, such as their heavy-tailed nature and dependence struc- tures. It is a potential technique for safe and dependable digital picture watermarking since the inclusion of a vector-based HMM further improves the watermark detector's accuracy. Through this work, we demonstrate the potential of combining advanced statistical models with wavelet transforms to achieve robust watermark embedding and detection, ensuring effective copyright protection and image integrity verification. Variance X is chosen for embeddings the watermark. watermarking factor is $\alpha$ .The proposed equation for embedding is given by $Y = X + \alpha W$ .Fig.1 illustrate the steps embedding the proposed watermarking method.

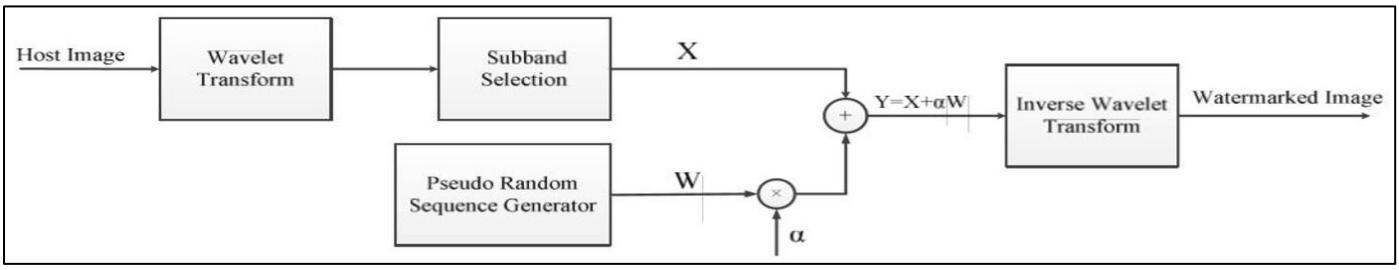


Fig 1 Embedding Procedure

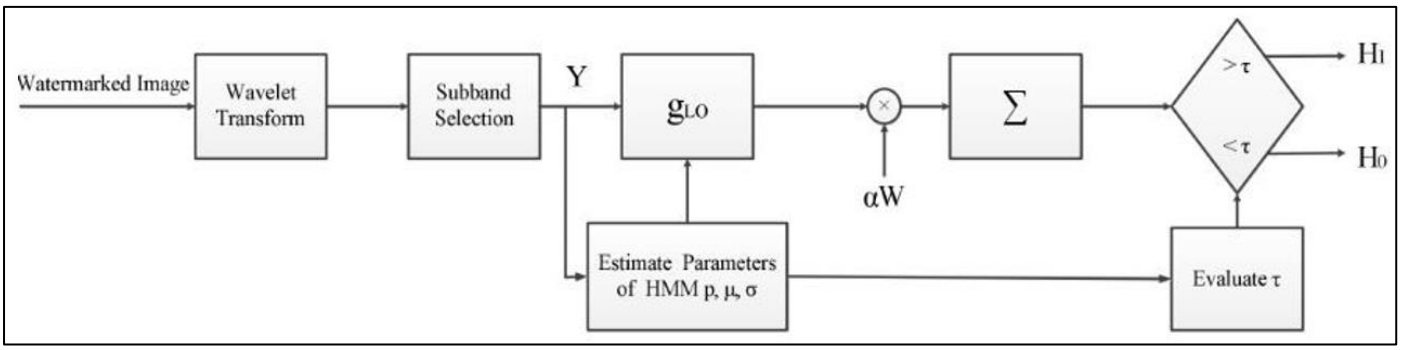


Fig 2 Local Optimum Wavelet Domain HMM Detector Procedure.

The detection procedure is show in Fig.1.Detector efficiency can be measured in terms of false alarm and detection probabilities, which lead to curves of the receiver operating characteristic (ROC).

In this paper, we used HMM model to build a locally opti- mal blind watermarking detector, which is a strong statistical model for the wavelet coefficients.In this model, account is taken of both the heavy-tailed characteristic and inter-scale and intra-scale dependencies between the wavelet coefficients.No visible variations in the experimental results between the host and the watermarked images suggest the characteristic of the proposed watermarking technique being strong imper- ceptibility.Improved watermarking detection efficiency of the proposed scheme compared with those obtained through the use of other wavelet coefficient models.

*B. Digital Watermark Extraction in Wavelet Domain using Hidden Markov Model.*

The watermark decoder plays a critical role in extracting the embedded secret bits of a watermark from digital me- dia. Leveraging the wavelet domain for watermark decoding provides significant advantages, particularly when employing a vector-based Hidden Markov Model (HMM). This advanced statistical model effectively captures the complex characteristics of wavelet coefficients, including their marginal distributions, inter-scale dependencies, and cross-orientation correlations. Such capabilities allow the vector-based HMM to offer a more precise representation of wavelet coefficients compared to traditional models, thereby improving the overall performance of watermark decoding.

The vector-based HMM is designed to model the dependencies within and across subbands of the wavelet transform. By capturing the heavy-tailed nature and dependency structures of wavelet coefficients, it ensures an accurate fit to the empirical data, outperforming previously adopted statistical distributions. This enhanced representation of wavelet domain statistics is fundamental in constructing a robust watermark decoder capable of withstanding various distortions and at- tacks.

Watermark Decoding in the Wavelet Domain The watermark decoder operates on the principle of maximum likelihood es- timation, ensuring that the extracted watermark bits maximize the likelihood of being present in the received signal. The theoretical framework for the decoder is derived in closed- form expressions, providing a solid mathematical foundation for its design and implementation. By optimizing the decoding process, the proposed watermark decoder achieves a significant reduction in bit error rates (BER) compared to conventional methods, particularly under challenging conditions such as noise, compression, or filtering.

The resilience of the proposed decoder to diverse forms of attacks highlights its robustness. This robustness is achieved by integrating the statistical modeling capabilities of the vector- based HMM with the multi-resolution analysis properties of the wavelet transform. Consequently, the decoder demon- strates superior performance in both controlled and adversarial scenarios, making it a reliable tool for secure watermark extraction.

➢ *Wavelet Domain Hidden Markov Model (HMM)*

A distribution with a large number of small coefficients and a small number of large coefficients is the inevitable outcome of an image's wavelet treatment. These coefficients fall into two categories: low-energy (small) and high-energy (big) states. For each wavelet coefficient, the vector-based HMM uses a two-state mixture model to simulate this distribution:

- *Small-Energy State:*

This state corresponds to Gaussian components with relatively small variances, effectively model- ing the peak around the mean value. Large-Energy State: This state captures the heavy tails of the coefficient distribution using Gaussian components with larger variances. By lever- aging this two-state HMM, the model captures both the peak and heavy-tailed characteristics of the wavelet coefficient distribution. The inter-scale dependencies and cross-orientation correlations are also explicitly modeled, enabling the decoder to make informed decisions during the watermark extraction process.

➢ *Superior Performance of the Proposed Decoder*

High levels of accuracy and robustness are guaranteed for the decoder with the incorporation of a vector-based HMM into the watermark decoding procedure. The maximum like- lihood criterion guarantees the best possible extraction of the watermark bits, while statistical modeling of wavelet coeffi- cients gives the decoder a solid theoretical basis. According to empirical findings, the suggested decoder routinely performs better than competing strategies in terms of bit error rates and resistance to frequent attacks.The target subband is selected using statistical analysis, and the watermark bits are included into certain subbands.

In summary, the proposed watermark decoder using a vector-based HMM in the wavelet domain offers a powerful solution for secure and reliable watermark extraction. Its ability to model the intricate statistical properties of wavelet coefficients, combined with its resilience to distortions, establishes it as a cutting-edge tool in the field of digital watermarking.Specific subbands contain the watermark bits; the target subband is selected using statistical analysis.

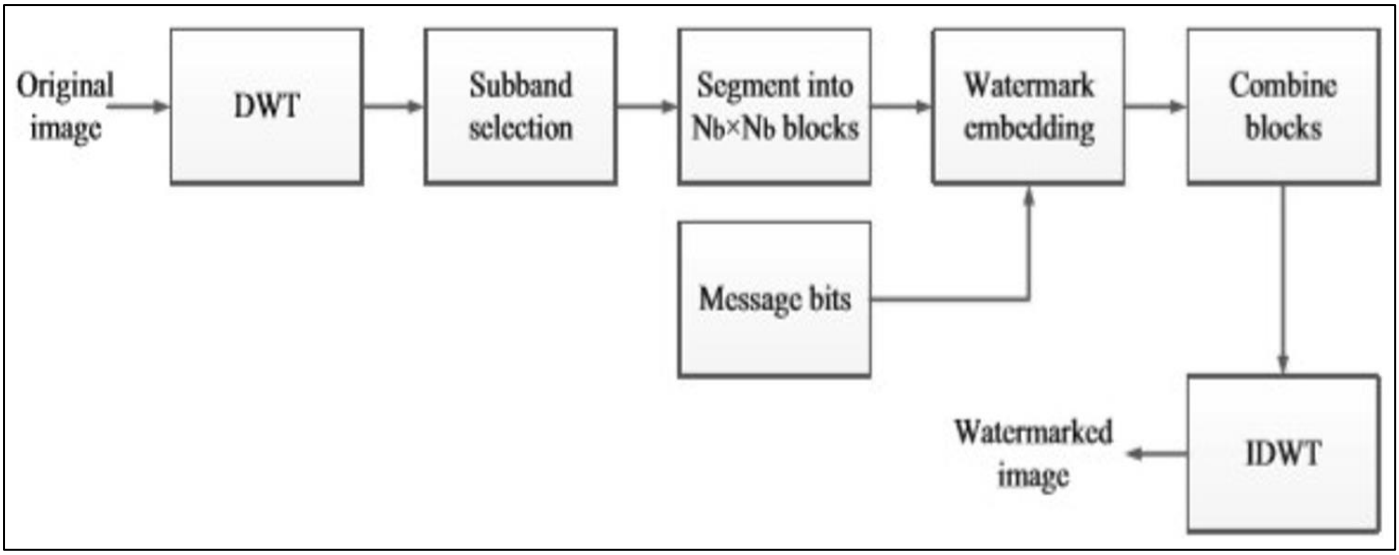


Fig 3 Embedding Part of the Proposed Watermarking Scheme.

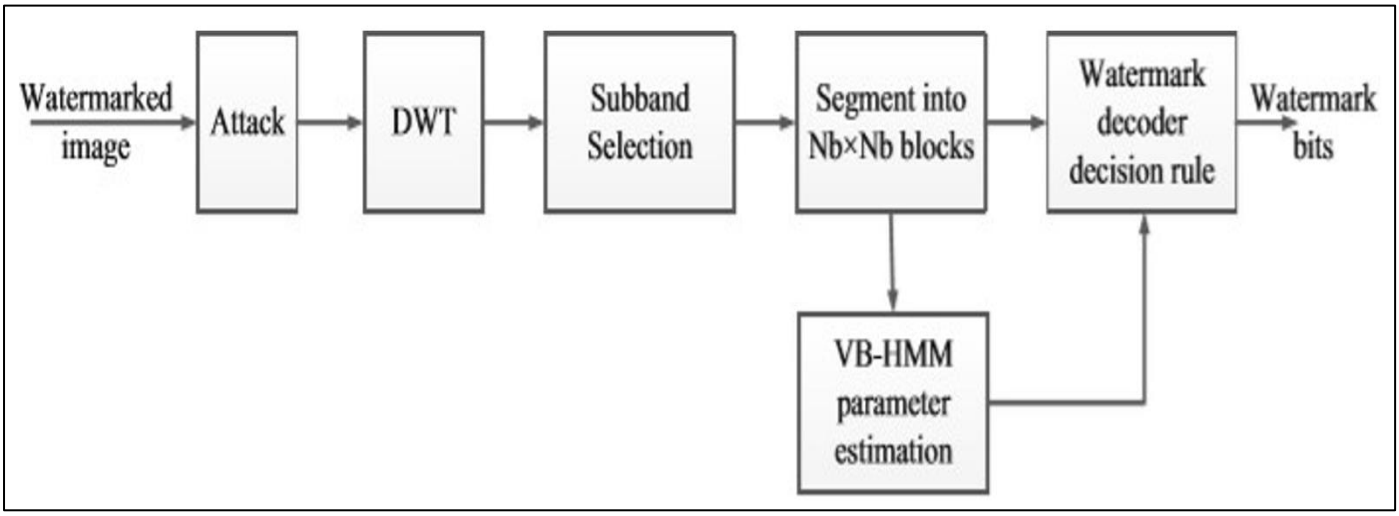


Fig 4 Extraction Part of the Proposed Watermarking Scheme.

Optimum blind watermark decoder using Wavelet domain vector-based HMM model.It has been shown that the vector- based HMM distribution is very similar to the distribution of image wavelet coefficients as it takes into account not only the heavy-tailed characteristics of these coefficients, but also the inter-scale and cross-orientation dependence between them. An optimal water-mark decoder was designed using the criterion of maximum probability. Closed-form expression for the decoder was obtained by using the vector-based HMM as a prior for the coefficients of the wavelet. The efficiency of the proposed watermark decoder was evaluated using a number of test images in terms of the bit error rate values. The proposed watermark decoder has been shown to be superior to other decoders in terms of having a lower rate of error on the bit. The proposed decoder based on the vector-dependent HMM has also been shown to be highly resilient against various types of attack.

*C. A Hidden Markov Model-based Blind Detector for Multiplicative Watermarking*

Blind detector in the wavelet domain for multiplicative watermarking images. To this end, the secret Markov model (HMM) based on the vector is used as a prior approximation for the host image's wavelet coefficients. This model is known to provide an effective fit to the wavelet coefficients distribution by capturing both their heavy-tailed marginal statistics as well as their inter-subbands and cross-orientation dependence. The performance of the proposed detector is shown to outperform that of the other detectors by providing the embedded watermark with a higher detection rate and greater imperceptibility. The proposed vector-based HMM detector is also shown to be more stable than other existing detectors under different attacks such as compression, rotation, filtering, and noise.

Watermarking guarantees the preservation of copyrights and security of digital data. It is realized by embedding in the host media a piece of information which can only be identified by the rightful owner of the intellectual property. Spatial embedding of the watermark can be done[8]. Wavelet coefficients were first modeled using the hidden Markov model (HMM) based on vectors in[9]. This simulation was realized by taking into account the non-Gaussianity of the coefficients of the wavelet image as well as the dependency between the orientations.

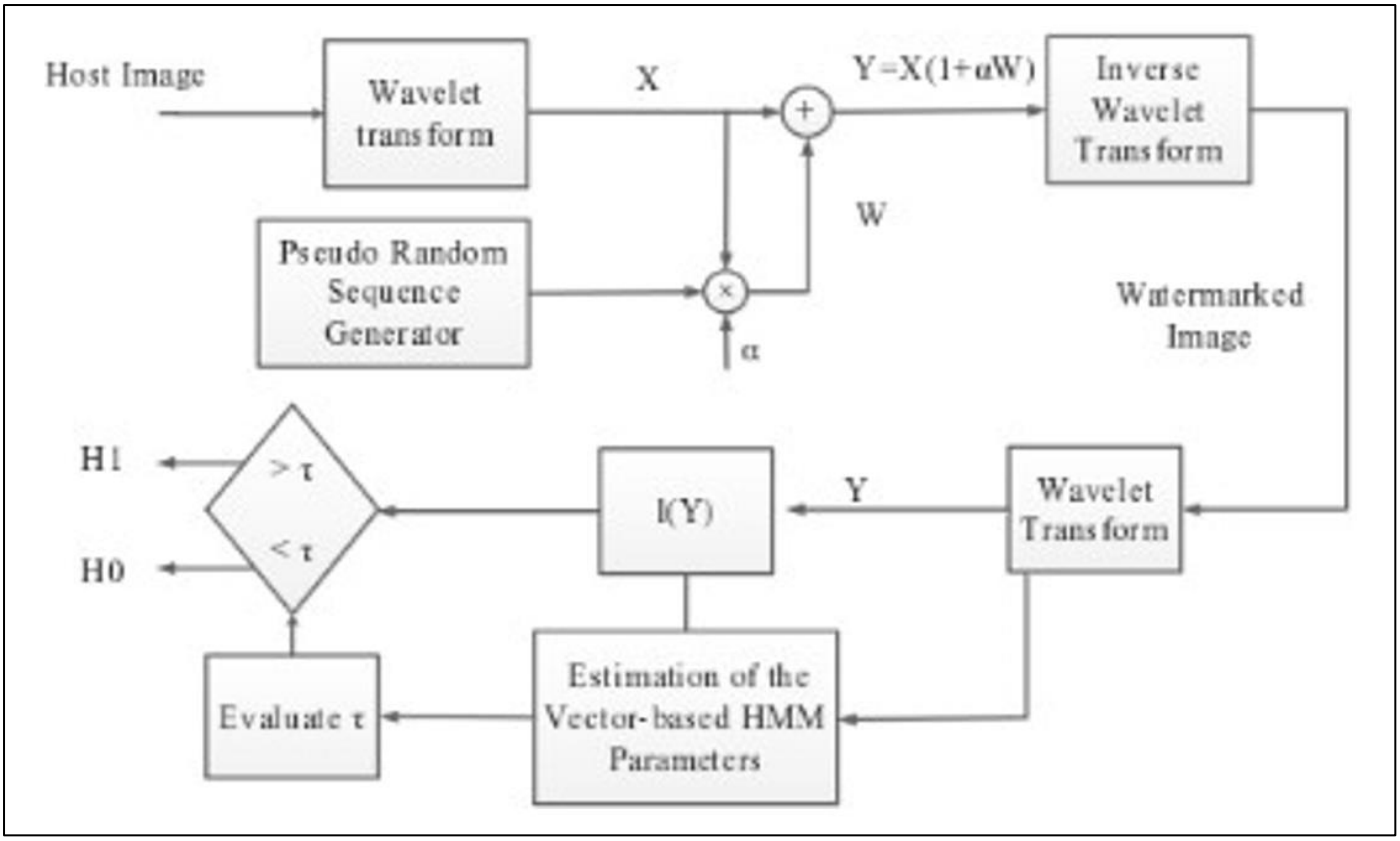


Fig 5 Proposed Watermarking Scheme; Embedding and Detection Parts.

The scheme proposed consists of two phases; embedding and detection. The watermark in the former is hidden in the host image, whereas the presence of the watermark is examined in the Fig. 5 Shows the schematics of both the proposed scheme's embedding and detection sections.

➢ *Multiplicative Watermark Embedding.*

Multiplicative watermarking method to conceal any piece of information in the host image. The grayscale image I of NI × NI is decomposed using a two-level wavelet transform.For hiding the watermark, subband X with the highest variance in the second level is chosen. The watermark W is generated using a pseudo-random sequence generator, taking equiprobable values {+1,-1} . Then the coefficients in subband X are updated according to the following multiplicative embedding approach as indicated by.

$$Y = (1 + \alpha W)X \tag{1}$$

Where α regulates watermark resistance. In other terms,α regulates the watermark's invisibility thus guaranteeing the watermarking scheme's robustness.The watermarked image is obtained by applying the inverse transform to the modified coefficients Y .Blind watermark identification, we take ad- vantage of the statistical characteristics of the wavelet image coefficients by using the HMM vector- modeling wavelet coefficients. Hypothesis testing is conducted to develop the watermark detector to verify whether the watermark exists or not. This check can be carried out as follows

$$H_1 : Y = (1 + \alpha W)X$$

$$H_0 : Y = X \tag{2}$$

Where $X = (x_1, x_2, \ldots, x_N)$ and $Y = (y_1, y_2, \ldots, y_N)$ are the chosen subband coefficients for the initial and n water- marked images respectively $W = (w_1, w_2, \ldots, w_N)$ is the watermark sequence and N is the number of the coefficients considered. The resulting watermarked images were shown to be less imperceptible than those resulting from the additive watermarking because of the data-dependent existence of the multiplicative watermarking.The multiplicative embedding method demonstrated senhanced watermark detection efficiency against various attacks compared to other existing detectors, including its additive equivalent, by providing higher water- mark detection levels with or without distortion.

*D. Blind Dual Watermarking for Color Images' Authentication and Copyright Protection*

The blind dual watermarking system designed for digital color images integrates two distinct watermarking techniques to serve different security purposes: a strong watermark for copyright protection and a weak watermark for image authentication. The first watermark, intended for copyright protection, is embedded into the YCbCr color space of the host image using the Discrete Wavelet Transform (DWT). This robust watermark can be extracted blindly, meaning it can be retrieved without requiring access to the original host image, providing a secure method for verifying ownership and preventing unauthorized use of the image.

In contrast, the second watermark, used for image authen- tication, is based on an enhanced Least Significant Bit (LSB) replacement approach. This fragile watermark is embedded within the RGB components of the image, which makes it particularly sensitive to image manipulation. Any alteration to the image, such as compression or cropping, will disrupt the fragile watermark, thus allowing for easy detection of tampering. This feature is particularly useful for

ensuring the integrity of the image and verifying that it has not been modified.

The dual nature of the system—combining robust watermarking for copyright protection and fragile watermarking for authentication—makes this approach highly effective in providing comprehensive security for digital images. The method ensures that both the ownership and the authenticity of the image can be verified independently, without the need for the original host image or watermark, thus offering a reliable solution for protecting valuable digital content against unauthorized use and tampering. The combination of these two watermarking techniques enhances the overall security framework, making it suitable for applications where both copyright protection and image authenticity are paramount.

Digital watermarking[10] is now a fairly focused technique aimed at providing a secure way to authenticate images or protect the security of copyrights; in this technique, a water- mark is generally invisibly inserted in the digital picture to avoid attracting malicious attackers attention. Digital water- marking techniques are divided into robust watermarking[11] and fragile watermarking[12], in keeping with the desired robustness of the embedded watermark.The main aim of the robust watermarking technique is mostly to secure host image ownership, while the weak watermarking technique is used to authenticate image integrity. Usually, robust watermarking is used to protect copyright, so it is designed to resist attacks that attempt to remove or damage the watermark without significantly degrading the visual quality of the watermark image.

In robust watermarking, verifiable user watermarks, such as logos or copyright information, are embedded within the host images. The primary objective is to allow verification of ownership by the inclusion of these watermarks. The process involves extracting the watermark from the watermarked image during verification, enabling the confirmation of the image's ownership. One of the primary concerns in robust watermarking is ensuring the watermark's resilience, meaning that the extracted watermark must remain intact and identifiable even after the image undergoes various signal processing attacks.

Fragile watermarking, on the other hand, is specifically designed for image authentication. The watermark in fragile watermarking is highly sensitive to alterations, meaning that even minor changes to the image (such as compression, cropping, or collage manipulation) will disrupt the watermark, making any modifications easily detectable. The integrity of the image can thus be verified by the presence or absence of the watermark.

In fragile watermarking, modifications to the host image—especially in less critical areas—result in significant degradation of the watermark's consistency. Consequently, the visual integrity of the fragile watermarked image is typically lower compared to robust watermarking, especially when the image is subjected to transformations that affect its quality. This sensitivity makes fragile watermarking a reliable method for detecting image tampering or manipulation.

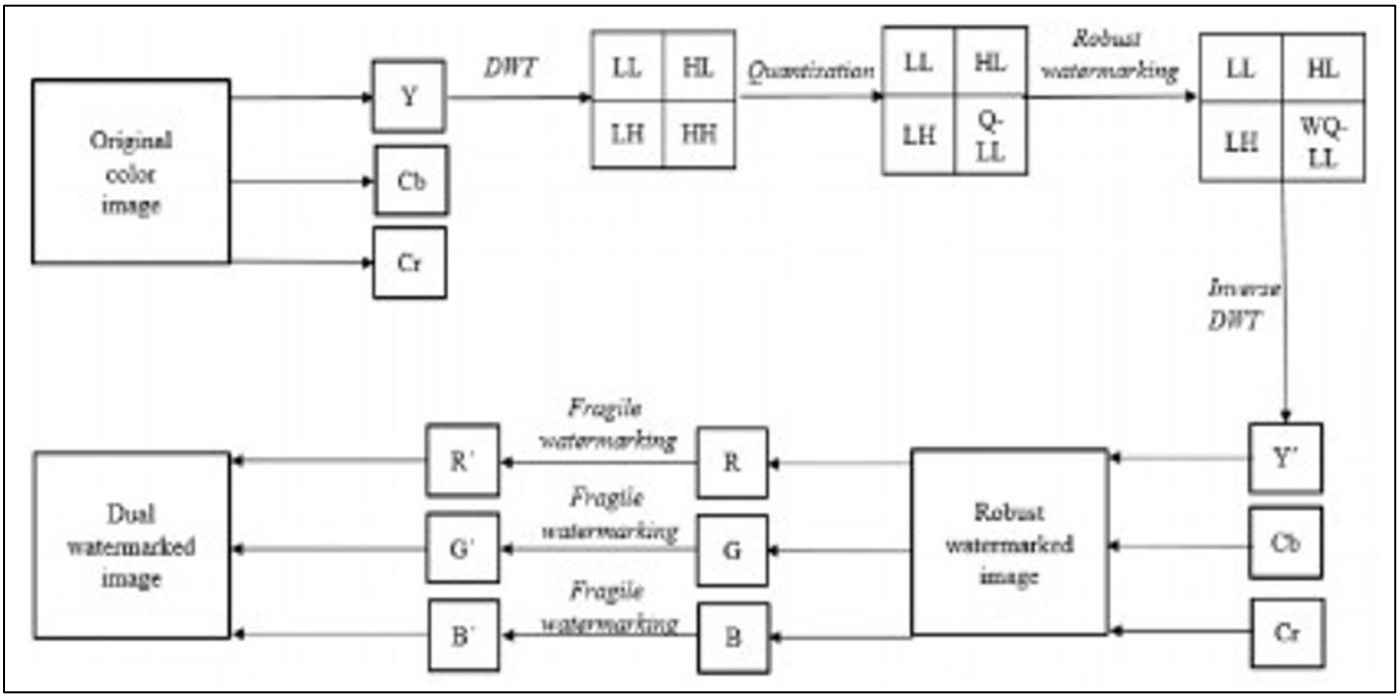


Fig 6 Watermark Embedding Procedure

A blind invisible dual watermarking system for color images is proposed to satisfy the image authentication and copyright protection requirements.

➢ *Dual Watermark Embedding*

The watermark embedding process is divided into two stages, i.e. 1) embedding the invisible stable watermark and 2) em- bedding the weak, invisible watermark.

- Phase 1: Embedding the invisible robust watermark The original RGB color picture is initially translated to color space YCbCr. The basic equations used for the transformation of RGB into YCbCr are:

$$Y = 0.299R + 0.587G + 0.114B$$

$$Cb = -0.172R - 0.339G + 0.511B + 128 \quad (3)$$

$$Cr = 0.511R - 0.428G - 0.083B + 128$$

After conversion of YCbCr, the one stage DWT decomposition of Y is performed to produce the low-low (LL), low-high (LH), high-low (HL) and high-high (HH) sub bands, where LL con- sists 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. Therefore we used this function for our robust watermarking scheme.Once the watermark is inserted, the inverse DWTs of the four corresponding sub-bands, i.e. LL, HL, LH, and WQ- LL, are performed to produce the Y 'watermarked path. The watermarked channels Y, 'Cb, and Cr are then converted back into RGB and saved as the robust watermarked image.

- Phase 2: Embedding the invisible fragile watermark After robust watermarking the robust watermarked color image is developed. Throughout this step, each RGB color channel of the robust watermarked image is independently embedded with the same fragile watermark (WF) for image authentica- tion.First, we convert the fragile watermark bit stream WF into a sequence of digits $W_F$ for each wave, i.e., R or G or B, by using a $3^n$-base notation system, where n is a parameter. Each digit in series $W_F$ is later viewed as one hidden digit s, which can be inserted into each channel's n-pixel unit U= ($p_1$, $p_2$, . . . , $p_n$).

Extraction of the Dual Watermark The robust watermark and the fragile watermark can be extracted separately for copyright detection and image authentication purposes, respectively, in the proposed extraction procedure. With respect to image au- thentication, the extraction of the fragile watermark is carried out separately by extracting three completed watermark bit streams in the watermarked image channel R, G and B.

Blind dual watermarking system for image identification and copyright protection in colour. The transparent, delicate, and durable watermarks are located within the RGB color space's spatial domain and within the YCbCr color space frequency domain.Watermarking mechanism can withstand various processing attacks and accurately position the manip- ulated area of the image. In addition, the dual watermarked image is imperceptible, making the proposed method ideal for safeguarding valuable original images. Comparison of the functionality of proposed mechanism with other, well known dual watermarking mechanisms

➢ *Comparison*

The comparison of the different Watermarking methods explained is presented in the below table.

## III. CONCLUSION

A comprehensive systematic review of various watermark- ing techniques has been conducted, highlighting the advance- ments in watermark detection methods. The analysis reveals that a novel multichannel watermark detection approach for color images was introduced, utilizing Hidden Markov Models (HMMs) to effectively model and capture the inter-channel dependencies present in the contourlet coefficients of color images. This method aims to improve the accuracy and relia- bility of watermark detection by accounting for the complex relationships between the color channels in the image.

Furthermore, the robustness of the proposed watermark-ing technique has been extensively evaluated across several types of image distortions and attacks, including compression, filtering, vibration, histogram modifications, and geometric transformations. The experimental results demonstrate that the proposed approach outperforms existing watermarking schemes in terms of robustness, making it more resilient to a wider range of common image manipulations and potential security threats.

Table 1 Comparison of Different Watermarking Methods

| Name | Method | Advantage | Disadvantage |
|---|---|---|---|
| New Blind Wavelet Domain Watermark Detector using Hidden Markov Model | vector-based hidden Markov model | Good imperceptibility of embedded watermark | Weak signal detection in non Gaussian noise. |
| Digital watermark extraction in wavelet domain using hidden Markov model | vector-based hidden Markov model | Low bit error rate | Embedding wa-termark in the sub band of the cover image.% |
| A Hidden Markov Model- based Blind Detector for Multiplicative Watermarking | Blind detector | Filter and noise more robust | Long time period of observation to reduce the error % |
| Blind dual watermarking for color images authentication and copyright protection | Discrete Wavelet transform | Accurately locate the tam- pered area of image | - |

## REFERENCES


[1]. M. Amini, M.O. Ahmad and M.N.S. Swamy, "A new blind wavelet domain watermark detector using hidden Markov model," in Proc. International Symposium on Circuits and Systems (ISCAS), pp. 2285- 2288,2014.

[2]. M. Amini, M.O. Ahmad and M.N.S. Swamy,"Digital watermark extrac- tion in wavelet domain using hidden Markov model," Multimedia Tools and Applications, vol. 75, no. 21, pp. 1-19, 2016.

[3]. M. Amini, H. Sadreazami, M.O. Ahmad and M.N.S. Swamy,"A hidden Markov model-based blind detector for multiplicative watermarking," in Proc. IEEE Midwest Symposium on Circuits and Systems (MWSCAS), pp.611-614, 2017.

[4]. X. L. Liu, C. C. Lin and S. M. Yuan, "Blind dual watermarking for color images' authentication and copyright protection," IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 5, pp. 1047- 1055,2016.

[5]. C. Wang, J. Ni and J. Huang,“An informed watermarking scheme using hidden Markov model in the wavelet domain,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 853-867, 2012.
[6]. M. Barni, F. Bartolini, A. DeRosa and A. Piva,“Color image water- marking in the Karhunen-Loeve transform domain,”Journal of Electronic Imaging, vol. 11, no. 1, pp. 87-95, 2002.
[7]. Crouse MS, Nowak RD, Baraniuk RG (1998),” Wavelet-based statistical signal processing using hidden Markov models,”IEEE Trans Signal Process 46(4):886–902.
[8]. I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon,“Secure spread spectrum watermarking for multimedia,”IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.
[9]. M. N. Do and M. Vetterli,“Rotation invariant texture characterization and retrieval using steerable wavelet-domain hidden Markov models,”IEEE Transactions on Multimedia, vol. 4, no. 4, pp. 517-527, 2002.
[10]. M. Yeung, F. Mintzer, “An invisible watermarking technique for im- age verification,”Proceedings of the International Conference on Image Processing, vol. 2, pp. 680-683,1997.
[11]. 5Q. Su, Y. Niu, H. Zou, X. X. Liu,“A blind dual color images water- marking based on singular value decomposition,”Applied Mathematics and Computation, vol. 219, no. 16, pp. 8455-8466, 2013.
[12]. C. S. Lu, H. Y. M. Liao,“Multipurpose watermarking for image authen- tication and protection,”IEEE Transactions on Image Processing,vol. 10, no. 10, pp. 1579-1592, 2001.