

A Robust Color Image Watermarking Algorithm with Various Attacks

K. Yashoda Kumari¹, Sumit Nema²

¹Student, Department of CSE, G.N.C.S.G.I., Jabalpur, India

²Professor, Department of CSE, G.N.C.S.G.I., Jabalpur, India

Abstract: The increased and widespread usage of digital multimedia has aroused great concerns regarding issues such as copyright protection, copy control and proof of ownership. Digital watermarking serves as a solution to these kinds of problems; however, with the help of my proposed Modified LSB watermarking embedding algorithm & watermark can easily be extracted in both clean and noisy environments. Experiments are performed to verify the robustness of the proposed algorithm. The results show that the proposed algorithm is superior to other algorithm in terms of providing a high PSNR. It is also shown that the proposed algorithm is highly robust against various kinds of attacks such as noise, filtering, cropping & rotation.

Keywords: Watermarked, PSNR, MSE, DWT, IDWT and RGB.

1. Introduction

As digital technologies have shown a rapid growth within the last decade, content protection now plays a major role within content management systems. Of the current systems, digital watermarking provides a robust and maintainable solution to enhance media security. The visual quality of host media (often known as imperceptibility) and robustness are widely considered as the two main properties vital for a good digital watermarking system. They are complimentary to each other and hence challenging to attain the right balance between them [5]. Digital image watermarking has become a necessity in many applications such as data authentication, broadcast monitoring on the Internet and ownership identification. Various watermarking schemes have been proposed to protect the copyright information. There are three indispensable, yet contrasting requirements for a watermarking scheme: robustness, invisibility and capacity. Therefore, a watermarking scheme should provide a trade-off between these features [2]. The security of digital information becomes an important concern in the digital multimedia era. As such a promising technique, digital watermarking is always one of the active research topics in the multimedia area. The basic idea is to embed auxiliary information into multimedia data, such as image, audio, video and text [1]. The rapid growth of visual media based applications necessitates sophisticated compression techniques in order to store, transmit and retrieve audio-visual information. The recent MPEG 4 and JPEG 2000 standards address the need for content based coding and manipulation of visual media. With the widespread use of the

Internet and the rapid and massive development of multimedia, there is an impending need for efficient and powerfully effective copyright protection techniques.

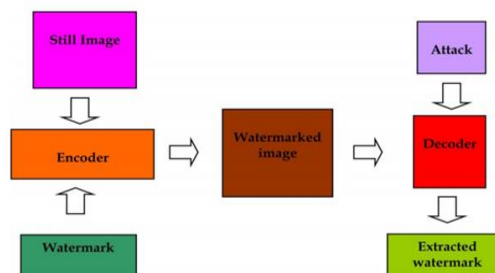


Fig. 1. Block diagram of the watermarking process

Digital watermarking schemes are typically classified into three categories. (1) Private watermarking which requires the prior knowledge of the original information and secret keys, at the receiver, (2) Semi-private or semi-blind watermarking where the watermark information and secret keys may be available at the receiver, and (3) public or blind watermarking where the receiver must only know the secret keys [7].

2. Literature review

Deepayan Bhowmik et.al: "Quality Scalability Aware Watermarking for Visual Content" In this paper, author propose a novel concept of scalable blind watermarking that ensures more robust watermark extraction at various compression ratios while not effecting the visual quality of host media. The proposed algorithm generates scalable and robust watermarked image code-stream that allows the user to constrain embedding distortion for target content adaptations. The watermarked image code-stream consists of hierarchically nested joint distortion-robustness coding atoms. The code-stream is generated by proposing a new wavelet domain blind watermarking algorithm guided by a quantization based binary tree. The code-stream can be truncated at any distortion-robustness atom to generate the watermarked image with the desired distortion-robustness requirements. A blind extractor is capable of extracting watermark data from the watermarked images. The algorithm is further extended to incorporate a bit-plane discarding-based quantization model used in scalable

coding based content adaptation, e.g., JPEG2000. This improves the robustness against quality scalability of JPEG2000 compression. The simulation results verify the feasibility of the proposed concept, its applications, and its improved robustness against quality scalable content adaptation. Our proposed algorithm also outperforms existing methods showing 35% improvement [1].

Matthew Oakes et.al: “*Visual Attention-Based Image Watermarking*” A new low complexity wavelet domain visual attention model is proposed that allows us to design new robust watermarking algorithms. The proposed new saliency model outperforms the state-of-the-art method in joint saliency detection and low computational complexity performances. In evaluating watermarking performances, the proposed blind and non-blind algorithms exhibit increased robustness to various natural image processing and filtering attacks with minimal or no effect on image quality, as verified by both subjective and objective visual quality evaluation. Up to 25% and 40% improvement against JPEG2000 compression and common filtering attacks, respectively, are reported against the existing algorithms that do not use a visual attention model [2].

Mohammed A. M. Abdullah et.al: “*A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography*” This paper presents a novel security architecture for protecting the integrity of iris images and templates using watermarking and Visual Cryptography (VC). The proposed scheme offers a complete protection framework for the iris biometrics which consists of two stages: the first stage is for iris image protection while the second is for the iris template. The experimental and comparison results on the CASIA V4 and UBIRIS V1 iris databases demonstrate that the proposed framework preserves the privacy of the iris images and templates and retains robustness to malicious attacks while it does not have a discernible effect on the recognition performance [3].

Xinshan Zhu et.al: “*Normalized Correlation-Based Quantization Modulation for Robust Watermarking*” A novel quantization watermarking method is presented in this paper, which is developed following the established feature modulation watermarking model. In this method, a feature signal is obtained by computing the normalized correlation (NC) between the host signal and a random signal. Information modulation is carried out on the generated NC by selecting a code word from the codebook associated with the embedded information. In a simple case, the structured codebooks are designed using uniform quantizes for modulation. The watermarked signal is produced to provide the modulated NC in the sense of minimizing the embedding distortion. The performance of the NC-based quantization modulation (NCQM) is analytically investigated, in terms of the embedding distortion and the decoding error probability in the presence of volumetric scaling and additive noise attacks. Numerical simulations on artificial signals confirm the validity of our analyses and exhibit the performance advantage of NCQM over

other modulation techniques [4].

3. Watermarking technique

In general digital watermarking involves two major operations: (i) watermark embedding, and (ii) watermark extraction. For both operations a secret key is needed to secure the watermark. The keys in watermarking algorithms can apply the cryptographic mechanisms to provide more secure services. The secret message embedded as watermark can almost be anything, for example, a bit string, serial number, plain text, image, etc. The most important properties of any digital watermarking technique are: robustness, security, imperceptibility, complexity, and verification. Watermarking techniques can be classified according to the nature of data (text, image, audio or video), or according to the working domain (spatial or frequency), or classified according to the human perception (robust or fragile). In images, the watermarking techniques can broadly be classified into three types: (i) visible watermark, (ii) invisible fragile watermark and (iii) invisible robust watermark, which has wider currency and use [5].

4. Proposed algorithm

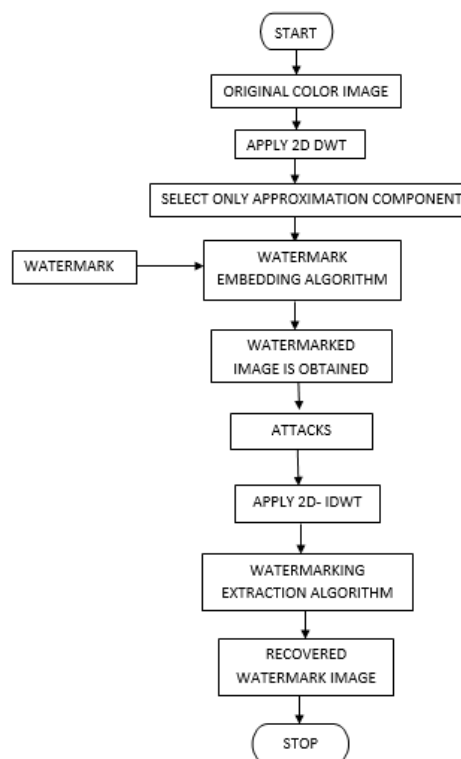


Fig. 2. Flow chart of watermarking algorithm

An image is a two dimensional signal containing a multitude of frequencies both high and low and is also represented as a two dimensional matrix. Therefore the most appropriate portion to be taken into account for watermark embedding consists of

high frequency components. So in order to identify the significant portion of the image data for consideration of watermark, the image I of size $M \times N$ is subjected to level 1 DWT thereby decomposed into four non overlapping multi-resolution sub-bands viz. LL (Approximation sub-band), HL (Horizontal sub-band), LH (vertical sub-band) and HH (diagonal sub-band), out of which LL is the low frequency component and rest are high frequency (detail) components. Apply watermarking embedding algorithm in Approximation sub-band so that watermarked image is obtained. When we want to extract the watermark apply IDWT on the watermarked image after than apply watermarking extraction algorithm so that watermark image is obtained.

5. Experimental results

Experiments are performed to evaluate the imperceptibility of the embedded watermark as well as the robustness of the proposed watermarking scheme against various attacks. In our experiments, we use color images of size 512×512 .

A. Invisibility of watermark

Invisibility is an evaluative measure of perceptual quality of the watermarked image. In a satisfactory image watermark algorithm, watermark should not cause much degradation of perceptual quality of the watermarked image. In the proposed algorithm, a watermark image is embedded into different test images to test invisibility. As shown in figure 3 & 4, there are not much visual differences between original test images and their corresponding watermarked images. The extracted watermarks are all easily distinguishable. Furthermore, by analyzing the absolute difference between the test image and the watermarked image the images are indistinguishable, thus showing the effectiveness of the proposed watermarking scheme in terms of the invisibility of the watermark.



Fig. 3. (a) Original and (b) proposed watermarked test images of Lena (c) Recovered watermarked

B. Robustness of the proposed algorithm

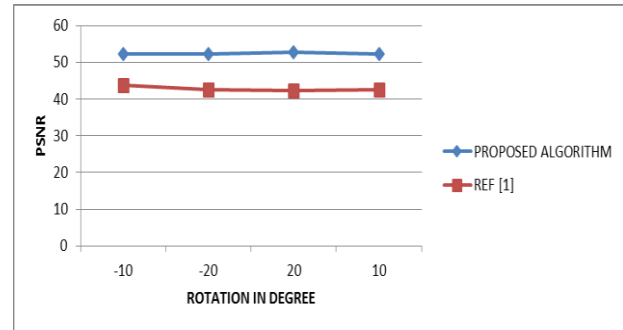


Fig. 4. Comparison of PSNR of LENA Image under the attack of "noise".

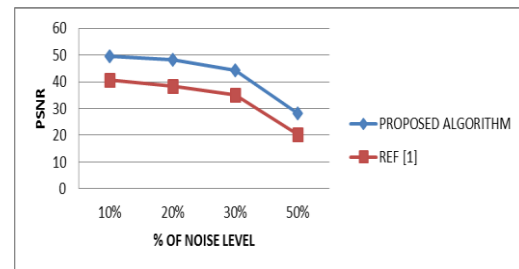


Fig. 5. Comparison of PSNR of LENA Image under the attack of "Cropping".

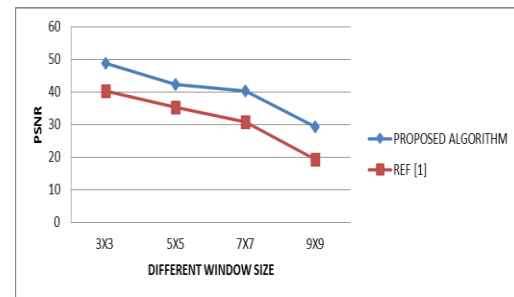


Fig. 6. Comparison of PSNR of LENA Image under the attack of "Rotation".

6. Conclusion

In this paper, a new proposed watermark detector has been proposed. Experiments have been carried out using standard color images to evaluate the performance of the proposed watermark algorithm. It has been shown that the performance of the proposed watermark algorithm for color images is substantially superior to that of the other conventional algorithm. It has been also shown that the performance of proposed algorithm is highly robust against common attacks such as salt & pepper noise, median filtering, cropping & rotation.

Table 1
 Performance of the Proposed Watermarking Scheme. The Best PSNR and MSE Values are Shown in Bold

IMAGES	PSNR(db)		MSE	
	Proposed Algorithm	REF[1]	Proposed Algorithm	REF [1]
Watermarked Image	55.39	50.23	0.223	0.393
Extracted watermark	54.66	44.67	0.324	0.786

Table 2
PSNR and MSE comparisons of test image 1 between the proposed scheme and the algorithm in [1] if rotation attack is present.










S. No.	ATTACK TYPE	PROPOSED WATERMARKED IMAGE		PROPOSED EXTRACTED WATERMARK		ALGORITHM [1] WATERMARKED IMAGE		ALGORITHM [1] EXTRACTED WATERMARK	
		PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
1	-10 Rotation	Watermarked Image 		Recovered Watermark 		Watermarked Image 		Recovered Watermark 	
		52.58	0.253	50.45	0.276	43.67	0.753	40.34	0.886
2.	-20 Rotation	Watermarked Image 		Recovered Watermark 		Watermarked Image 		Recovered Watermark 	
		52.31	0.261	49.23	0.291	42.67	0.812	39.13	0.976
3.	20 Rotation	Watermarked Image 		Recovered Watermark 		Watermarked Image 		Recovered Watermark 	
		52.76	0.298	49.67	0.288	42.24	0.874	39.65	0.926
4.	10 Rotation	Watermarked Image 		Recovered Watermark 		Watermarked Image 		Recovered Watermark 	
		52.31	0.261	49.23	0.291	42.67	0.812	39.13	0.976

Table 3
 PSNR and MSE comparisons of test image 1 between the proposed scheme and the algorithm in [1] if noise attack is present.

S. No.	ATTACK TYPE	PROPOSED WATERMARKED IMAGE		PROPOSED EXTRACTED WATERMARK		ALGORITHM [1] WATERMARKED IMAGE		ALGORITHM [1] EXTRACTED WATERMARK	
		PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
1	10 % SPN	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		49.31	0.292	45.34	0.691	40.66	0.812	38.34	1.076
2.	30 % SPN	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		48.46	0.332	42.34	0.711	38.23	1.034	35.34	2.716
3.	50 % SPN	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		44.16	0.692	38.45	1.12	35.23	2.134	29.34	12.26
4.	70 % SPN	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		26.45	12.78	25.29	13.78	24.32	15.512	20.24	15.116

Table 4
PSNR and MSE comparisons of test image 1 between the proposed scheme and the algorithm in [1] if cropping attack is present.









S. No.	ATTACK TYPE	PROPOSED WATERMARKED IMAGE		PROPOSED EXTRACTED WATERMARK		ALGORITHM [1] WATERMARKED IMAGE		ALGORITHM [1] EXTRACTED WATERMARK	
		PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
1	10 % cropping	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		52.58	0.253	50.45	0.276	43.67	0.753	40.34	0.886
2.	20 % cropping	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		52.18	0.283	49.91	0.296	43.67	0.756	40.34	0.886
3.	30 % cropping	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		51.08	0.323	50.45	0.276	42.15	0.779	38.23	1.216
4.	40 % cropping	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		48.78	0.979	46.21	1.081	42.34	1.12	23.12	18.34

Table 5
 PSNR and MSE comparisons of test image 1 between the proposed scheme and the algorithm in [1] if filtering attack is present.

S. No.	ATTACK TYPE	PROPOSED WATERMARKED IMAGE		PROPOSED EXTRACTED WATERMARK		ALGORITHM [1] WATERMARKED IMAGE		ALGORITHM [1] EXTRACTED WATERMARK	
		PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
1	3 X 3 MF	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		48.78	0.979	46.21	1.081	40.34	1.212	32.12	5.676
2.	5 X 5 MF	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		42.15	1.679	32.25	5.081	35.34	7.112	30.12	17.76
3.	7 X 7 MF	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		40.23	1.23	20.12	24.23	30.67	34.22	18.23	50.12
4.	9 X 9 MF	Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur		Watermarked Image 		Recovered Watermark Global Nature Care Sangathan's Group of Institutions Jabalpur	
		29.23	9.45	20.34	25.29	19.23	65.24	14.34	93.11

References

[1] Deepayan Bhowmik et.al: "Quality Scalability Aware Watermarking for Visual Content" IEEE Transactions On Image Processing, vol. 25, no. 11, November 2016.

[2] MATTHEW OAKES et.al: "Visual Attention-Based Image Watermarking" IEEE access November 9, 2016.

[3] Mohammed A. M. Abdullah et.al: "A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography" IEEE Access 2016, page no. 2169-3536.

[4] Xinshan Zhu et.al: "Normalized Correlation-Based Quantization Modulation for Robust Watermarking" IEEE Transactions On Multimedia, vol. 16, no. 7, November 2014, page no. 1888-1905.

[5] Hamidreza Sadreazami et.al: "Multiplicative Watermark Decoder in Contourlet Domain Using the Normal Inverse Gaussian Distribution" IEEE Transactions On Multimedia, vol. 18, no. 2, February 2016.

[6] Gamal Fahmy et.al: "Joint Watermarking and Compression for Images in Transform Domain" International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.4, July-Aug. 2012 pp. 2341-2351.

[7] Mustafa Osman Ali et.al, "Invisible Digital Image Watermarking in Spatial Domain with Random Localization" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 5, November 2012.