A Robust, Non-blind High Capacity & Secure Digital Watermarking Scheme for Image Secret Information, Authentication and Tampering Localization and Recovery via the Discrete Wavelet Transform

S. S. Chaughule, and D. B. Megherbi

CMINDS research center, Department of Electrical and Computer Engineering, University of Massachusetts, Lowell, U.S.A

***Abstract* — In today's world accessibility and trade of advance digital information over the web is of key significance. *Security and verification of digital information*, including digital images, is one of the greatest concerns. For this specific reason, in this paper we propose a *non-blind* watermarking technique for self-recovery and authentication of hidden images against unauthorized tampering by utilizing the Discrete Wavelet Transform (DWT) and the Arnold's Transform. Due to the nature of the Discrete Wavelet Transform, DWT-based watermarking schemes, in general, have the hidden images size limited to up to ¼ of the carrier image size; that is, for example, for a 256x56-carrier image the size of the hidden images is usually up to 128x128. In this paper, we show how the proposed DWT-based technique (a) has a moderately high capacity capability as it allows hidden images of the same size as that of the carrier image, (b) uses a self-recovery framework for watermarking and information hiding that allows embedding twice the number of correction matrices as in prior related work. *This makes the proposed non-blind technique equipped with about twice as much capability of self-recovery from unauthorized tampering as in prior work,* (c) allows unauthorized tampering localization and recovery against unauthorized tampering such as image cropping, blurring, pixel tampering, (d) utilizes all three-color channels of a carrier image for watermarking and information hiding, and (e) adds security in the secret hidden image information. Experimental results are presented to show the potential value of the proposed non-blind method for multiple information hiding of same size and the carrier image, tampering detection/localization, authentication, and tampering self-recovery, including cropping, and robustness of the proposed scheme to JPEG compression and encryption, and other unauthorized tampering.**

***Index Terms*— Watermarking, Chaotic Map, DWT, Arnold Transform, Tampering, Recovery**

I. Introduction

In today's world of intense communication, internet has turned into the most essential source of information trade. And with increase in speed and accessibility of internet it is getting even simpler and simper day by day. With such technological advancements of the applications over the internet has significantly caused concerns about the robustness and ownership of the traded information. In order to secure the robustness and to protect the ownership of the digital information digital watermarking can be utilized.

Watermarking is defined as a process of embedding digital information known as watermark in a host signal [1]. In order to authenticate the robustness of data and to check its copyright information, the embedded watermark signal is extracted at the receiving end [7].

II. Related Work

In [2], Khare, Verma, and Srivastava utilized DWT and chaotic transformation for watermarking, but their technique is limited to embedding a single watermark image. Subsequently, in [4] Singh, Rawat, and Agrawal utilized the properties of both DWT's and DCT's which gives them an upper hand over attacks such as filtering and compression.

In [7] Potdar, Han, and Chang survey various digital watermarking techniques and discuss a comparison between different frequency domains watermarking techniques. In [8], Garcia, Reyes, Ponomaryov, and Ramos suggested an approach, to recover the watermark image and authenticate the carrier image using an authentication matrix. Saha, Pradhan, Kabi, and Bisoi [10] suggested a watermarking algorithm using DWT, RSA and Arnold's Transform making their technique relatively more secure.

Some of the constraints of these strategies are that they suffer from the restrictions of capacity of data that can be inserted. These schemes, in general, do not sustain cropping attacks, as their limitation on capacity limit them from inserting information which could be useful to recover from cropping.

In [20], we focused around accomplishing a non-blind watermarking algorithm, which had a relatively high capacity, high redundancy, recoverable and secure. In [20], we accomplished high capacity by embedding the information in DWT coefficients. However, we were embedding two grayscale images of a quarter size of that of the carrier image size. We also achieved recovery, by extracting the correction matrices and using them with the correction algorithm described in [20] to recover the tampered information. The high redundancy was obtained by strategically embedding the information in all three-color channels. Subsequently, in [19] we proposed a *blind* watermarking technique, which does not require a watermark at the receiving end for authentication. In [19] the information redundancy of the technique is less than that of the technique proposed in [20], but the capacity of the technique mentioned in [19] is relatively higher than that in [20].

In this paper, we focus on achieving a higher capacity and redundancy as compared to the techniques suggested in [20] and [19], by using a non-blind scheme. Here we embed a watermark image and a secret hidden image of the same size as that of the carrier image*, and embed twice the number of*

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

correction/recovery matrices, which makes this techniques twice as much recoverable as compared to the technique mentioned in [20] and [19].

In this paper, we describe the proposed technique in the first section. In the second section, we present the experimental results of the technique and its robustness to several unauthorized attacks, including cropping, tampered pixels, jpeg compression, noise, and encryption. In the last section, we present our conclusions.

III. THE PROPOSED METHODOLOGY

The embedding and the extraction algorithms in the proposed technique are explained in Table-1 and Table-2. Similar to the technique suggested in [19], we embed combination matrices of hidden and watermark images in two color channels of the host image and recovery/correction matrices in the third channel of the host image. Similar to [20], the hidden image is encoded using Arnolds transform and then embedded in DWT bands using the combination matrix. The high redundancy is obtained by strategically placing the correction matrices in the DWT bands of the third channel.

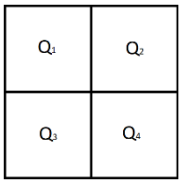

Fig. 1. Decomposition of Image into quadrants

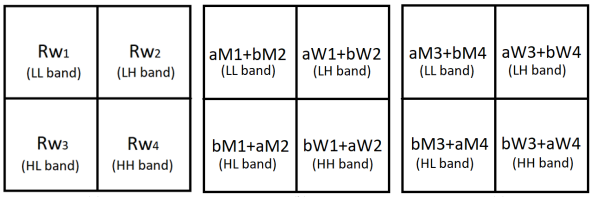

Fig. 2. DWT decomposition of the host image for embedding a secret hidden image (M1, M2, M3 & M4), a watermark image (W1, W2, W3 & W4) and correction matrices (Rw1, Rw2, Rw3 & Rw4)

TABLE I. Proposed embedding algorithm for scheme

Proposed Watermarking Embedding Scheme
Step 1: Obtain the RGB color planes of the host image.
Step 2: Apply one level of DWT decomposition for all the color planes as shown in Fig. 2.
Step 3: Obtain a correction matrix of the original hidden image as described in [20].
Step 4: Divide both the hidden and watermark image into four quadrants as shown in Fig. 3 and as described in [19].
Step 5: Apply Arnold's Transform to the hidden image with 'I' number of iterations.
Step 6: Obtain the respective combination images such as 'aM1+bM2' as shown in Fig. 2 and described in [19].
Step 7: Embed a hidden and a watermark images in their respective bands of the host channels as shown in Fig. 2.
Step 8: Change the alignment or orientation of the correction matrices such that it is a multiple of 90 degree for each band, to increase robustness to cropping of the technique.
Step 9: Embed the correction matrices in their respective band as in Fig. 2.
Step 10: Apply inverse DWT

TABLE II. Proposed extracting algorithm for scheme

Proposed Watermarking Extracting Scheme
Step 1: Obtain RGB color planes of the watermark image.
Step 2: Apply one level DWT decomposition to the watermarked image.
Step 3: referring to Figure 2 (b) and (c) derive the two images from the host image.
Step 4: Iterate the hidden image using Arnold's Transform in order to get the original image.
Step 5: Authenticate the watermark image for any tampering.
Step 6: Extract the correction matrices embedded in the third band and illustrated in Figure 2 (a).
Step 7: Correct the alignment of the correction matrices.
Step 8: Apply the correction algorithm, as discussed in [20], if tampering is detected in step (5).

A. Experimental Results of the Proposed Scheme

In this section, we present the experimental results of proposed technique. Images shown in Fig. 3 (a), (b) and (c) are carrier, watermark, and secret hidden images respectively. Here the size of each the carrier, the watermark and the hidden images is 256X256 respectively.

Fig. 3. Examples of images used in our experiments. (a) Carrier image, (b) Grayscale secret hidden image, (c) Watermark image

Effect of Partial Blurring on the Proposed Scheme

Here the watermarked image is blurred partially to observe the effect of tampering over the extracted or recovered images.

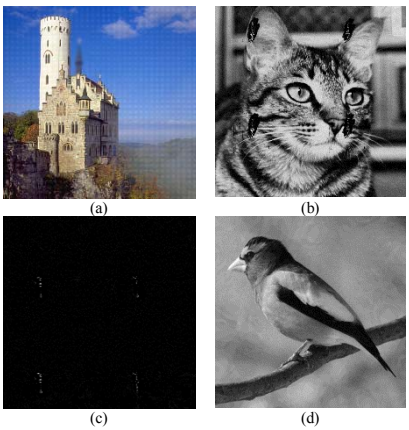

Fig. 4. Effect of partial image blurring. (a) Watermarked image exposed to a partial image blurring attack, (b) Watermark image extracted, (d) Authentication image, (c) Final extracted hidden image, using the proposed correction algorithm

Effect of Pixel Tampering:

Here a 64X64 image of a man is placed inside the watermarked image to observe the resulting effect on the extracted or recovered images.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

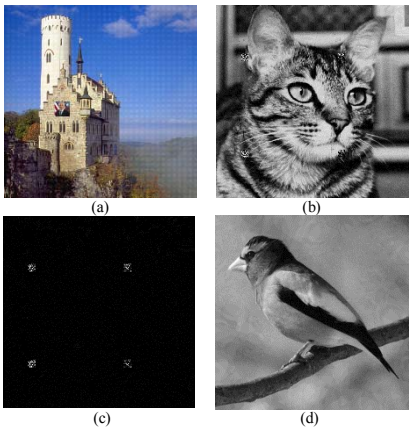

Fig. 5. Effect of image pixels tampering. (a) Watermarked image exposed to Tampering, (b) Watermark image, (c) Authentication image, (d) Final extracted hidden image.

Effect of Salt & Pepper Noise:

Results in the case when salt and pepper noise is added spatially to a whole watermarked image.

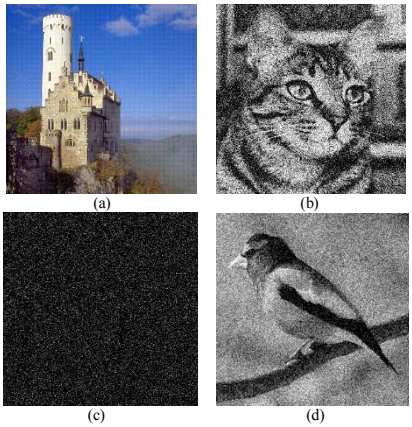

Fig. 6. Effect of salt & pepper noise: (a) Watermarked image exposed to salt & pepper noise, (b) Watermark image, (c) Authentication image, (d) Final extracted image (PSNR = 27 dB)

Effect of JPEG Compression:

Figures 7 and 8 present the effect of JPEG compression, with varying degrees of lossy compression, on the resulting hidden images in the cases when the extracted hidden image is corrected using the proposed algorithm and when it is not corrected, respectively.

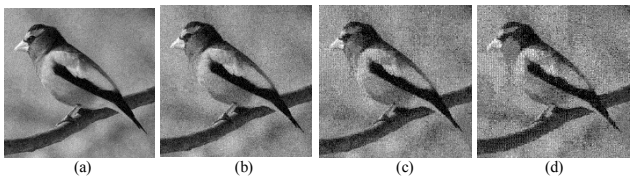

Fig. 7. Effects of JPEG compression at different quality factors (QF) when the extracted hidden image is corrected using the proposed correction algorithm. (a) Final extracted hidden image (PSNR = 29dB) when QF = 100, (b) Final extracted hidden image (PSNR = 25dB) when QF = 98, (c) Final extracted hidden image (PSNR = 21dB) when QF = 96, (d) Final extracted image (PSNR = 19dB) when QF = 94.

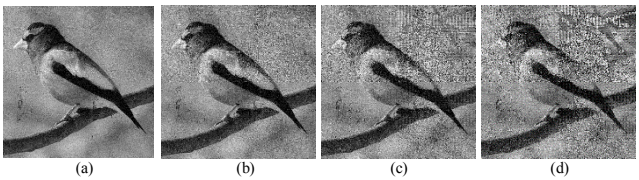

Fig. 8. Effects of JPEG compression at different QF when the extracted hidden image is not corrected. (a) Extracted hidden image (PSNR = 28dB) when QF = 100, (b) Extracted hidden image (PSNR = 22dB) when QF = 98, (c) Extracted hidden image (PSNR = 14dB) when QF = 96, (d) Extracted final image (PSNR = 12dB) when QF = 94.

Effect of Encryption:

Here, for increased security, the hidden image is scrambled using Data Encryption Standards (DES) algorithm, then again encoded using the Arnold's transform.

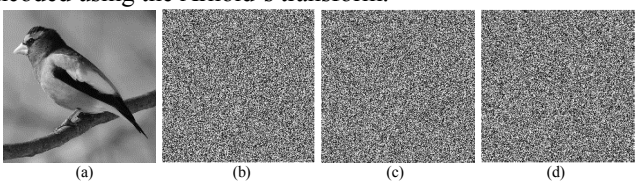

Fig. 9. Effects of DES encryption. (a) Original hidden image, (b) Encrypted hidden image, (c) Extracted encrypted hidden image, (d) Decrypted hidden image

Effect of the Nature of the Carrier and Hidden Images:

Here, we are observing the effect of the scheme on different variety of carrier and hidden images.

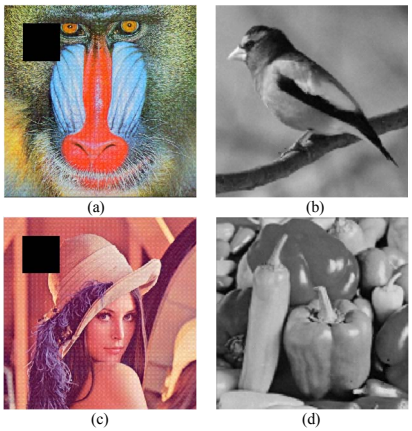

Fig. 10. Examples of different natures of host and hidden image used to test the proposed scheme. In general the scheme resulted in good quality of the recovered hidden images after cropping attacks: (a), & (c) are Tampered Watermarked Carrier Image for hidden images (b), & (f) respectively.

Further Analysis of the Robustness of the Proposed Scheme

Fig. 11 demonstrates a graph of the PSNR value of the extracted watermark image, against the percentage of error (tampering) done on the pixels of the watermarked image. As one may observe in Fig. 11, the PSNR value of the extracted and corrected hidden image remains above 30 dB at 50%-pixel tampering/error in the watermarked carrier image.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

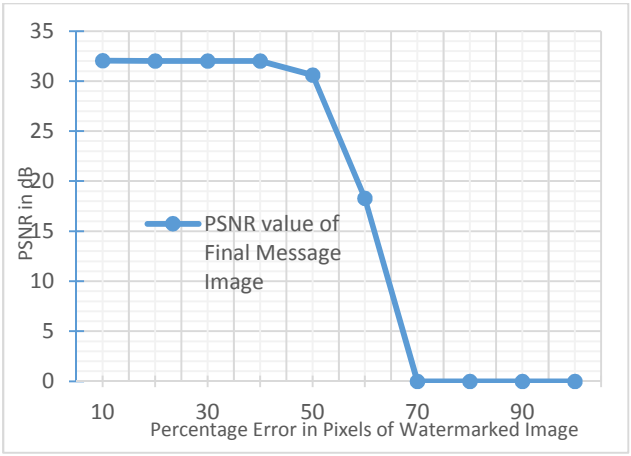

Fig. 11. Plot of the PSNR of the final extracted watermark image against percentage of error in the pixels of the watermarked image (fully embedded carrier).

Fig. 12 represents a graph of the PSNR value of the extracted watermark image as well as the watermarked image against the density of salt and pepper noise added to the watermarked image. As one may observe, at a noise density value of 0.0025, the PSNR value of the extracted watermark image remains above 30 dB.

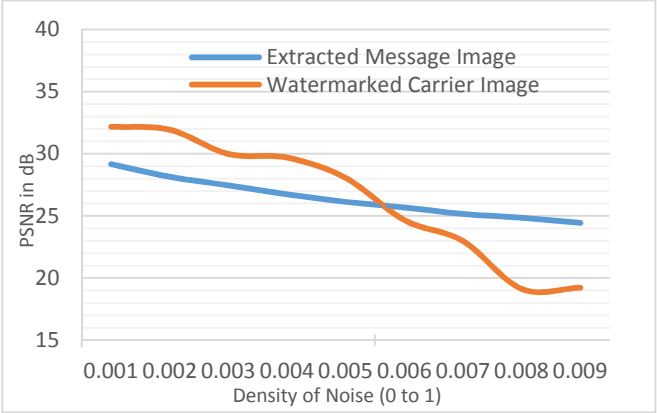

Fig. 12. Plot of the PSNR values of the final extracted watermark image and watermarked image against the density of salt-pepper noise added to the watermarked carrier image.

IV. Conclusion

In this paper, we proposed a non-blind, robust, secure and relatively high capacity image-watermarking scheme. The proposed scheme has achieved a relatively high capacity and error correction by adapting the pros of the techniques mentioned in [19] and [20]. The advantage of the related techniques in [19][20] is their being blind and not requiring knowledge of the image watermark at the receiver's end. By using redundancy in the embedded error correction/recovery matrices, the proposed technique generally provides relatively about twice as much capability of self-recovery from unauthorized tampering as in prior related work.

References

[1] Vinayak S. Dhole and Nitin N Patil, "Self-Embedding Fragile Watermarking for Image Tampering Detection and Image Recovery using Self Recovery Blocks" , Computing Communication Control and Automation, International Conference, India, July 2015.

[2] Priyank Khare, Alok Kumar Verma and V. K. Srivastava, "Digital Image Watermarking scheme in Wavelet Domain using Chaotic Encryption" Engineering and Systems (SCES), 2014 Students Conference, India, August 2014.

[3] Nikodim Lazarov and Zlatoliliya Ilcheva, "A Fragile Watermarking Algorithm for Image Tamper Detection Based on Chaotic Maps", Intelligent Systems (IS), 2016 IEEE 8th International Conference, Bulgaria, September 2016.

[4] Surya Pratap Singh, Paresh Rawat and Sudhir Agrawal, "A Robust Watermarking Approach using DCT-DWT" , International Journal of Emerging Technology and Advanced Engineering, Vol. 2, August 2012.

[5] Madhuri Rajawat and D. S. Tomar, "A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT", Communication Systems and Network Technologies, 2015 Fifth International Conference, April 2015.

[6] Ravi K Seth and Dr. V. V. Nath, "Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete wavelet Transform method", Advances in Computing, Communication, & Automation, IEEE International Conference, September 2016.

[7] Vidyasagar M. Potdar, Song Han and Elizabeth Chang, "A Survey of Digital Image Watermarking Technique", Industrial Informatics, 2005. INDIN '05. 2005 3rd IEEE International Conference, December 2005.

[8] Javier Molina-Garcia, Rogelio Reyes-Reyes, Volodymyr Ponomaryov and Clara Cruz-Ramos, "Watermarking Algorithm for Authentication and Self-Recovery of Tampered Images Using DWT" , Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW), 9th International Kharkiv Symposium, Ukraine, August 2016.

[9] Mohammad Abdullatif, Othman Khalifa, R.F. Olenrewaju, Akram Zeki, "Robust Image Watermarking Scheme By Discrete Wavelet Transform", Computer and Communication Engineering (ICCCE), 2014 International Conference, Malaysia.

[10] Bidyut Saha, Chittaranjan Pradhan, Kunal Kabi, Ajay Bisoi, "Robust Watermarking Techniques using Arnold's Transformation and RSA in Discrete Wavelets", Information Systems and Computer Networks (ISCON), 2014 International Conference, India, 2014.

[11] Meeta Malonia, Sureshra Agarwal, "Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression Technique" , Electrical, Electronics and Computer Science, 2016 IEEE Students' Conference, India, July 2016.

[12] Sin-Joo Lee, Sung-Hwan Jung, "A Survey on Watermarking Techniques Applied to Multimedia", Industrial Electronics, 2001. Proceedings. ISIE 2001. IEEE International Symposium, South Korea, June 2001.

[13] S. Voloshynovskiy, F. Deguillaume, T. Pun, "Content Adaptive Watermarking Based On Stochastic Multi-resolution Image Modelling", Signal Processing Conference, 2000 10th European, Finland, Sept. 2000.

[14] P. Tao, A. Eskicioglu, "A robust multiple watermarking scheme in the Discrete Wavelet Transform Domain", Symposium on

Internet Multimedia Management Systems, Philadelphia, PA. October 25-28, 2004.

[15] M. Raval, P. Rege, “Discrete Wavelet Transform Based Multiple Watermarking Scheme”, TENCON 2003. Conference on Convergent Technologies for the Asia-Pacific Region, India.

[16] A. Singh, J. Nigam, R. Thakur, R. Gupta, A. Kumar, “Wavelet Based Robust Watermarking Technique for Integrity Control in Medical Images” , Micro-Electronics and Telecommunication Engineering (ICMETE), 2016 International Conference, India, June 2017.

[17] N. Wang, C. H. Kim, “Tamper Detection and Self-Recovery Algorithm of Color Image Based on Robust Embedding of Dual Visual Watermarks Using DWT-SVD”, Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium, South Korea, December 2009.

[18] S. Qiang, Z. Hongbin, “Color Image Self-Embedding and Watermarking Based on DWT”, Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference, China, May 2010.

[19] S. Chaughule , D. B. Megherbi, “A Robust Double-Blind Secure High Capacity Watermarking and Information Hiding Scheme For Authentication and Tampering Recovery Via the Wavelet and Arnold Transforms”, 2018 IEEE International Symposium on Technologies for Homeland Security (HST), October 2018.

[20] S. Chaughule, , D. B. Megherbi, “A Robust Secure and High Capacity Image Watermarking Scheme for Information Exchange in Distributed Collaborative Networked Intelligent Measurement Systems”, 2018 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA).

978-1-7281-5092-5/19/$31.00 ©2019 IEEE