Image Watermarking based on Non-Newtonian Effect and Interpolated SWT-DWT

Ahmed Khan and KokSheik Wong
School of Information Technology, Monash University Malaysia, Malaysia.
E-mail: {ahmed.khan1,wong.koksheik}@monash.edu

***Abstract*—This paper proposes a robust image watermarking method based on the non-Newtonian effect in fluid dynamics and multiple interpolated transformations. First, the host image is encrypted by using a k-level Arnold map, followed by Discrete Wavelet Transformation. Second, the watermark is inserted into the encrypted-transformed host image, where the resulting image is inversely transformed by using inverse stationary wavelet transformation, followed by the inverse Arnold mapping (decryption) to produce the watermarked image. Specifically, inserting watermark into the Arnold domain diffuses the watermark information throughout the host image, which leads to the non-Newtonian effect. All three color channels of the host image are processed differently to achieve robust watermark extraction and quick tampering detection. Experiments are conducted to verify the basic performance of the proposed method. Results suggest that the proposed method outperforms the conventional work in terms of image quality while achieving high robustness and embedding capacity.**

I. Introduction

Nowadays digital content can be easily produced and distributed thanks to the availability of advanced smart devices and user-friendly yet effective content editing software. However, it is for the same reason that numerous threats are linked to the ownership of content especially for artists, content providers, government data, and lately researchers as well due to the need of large volume of data for training various machine learning models [1]. Therefore, watermarking methods are developed by many researchers to prevent these valuable contents from various forms of attack [2]. Specifically, in the case of images, a digital watermark is commonly embedded into the host with the aim to survive various forms of image processing operations targeted for the removal of watermark. On the other hand, various attacks are designed to remove or alter the watermark embedded into a host so that the watermark extraction process (from the attacked image) eventually fails [1].

Throughout the years, researchers explored numerous techniques to achieve robust watermarking in the spatial and frequency domains. In the spatial domain, various innovations are put forward, including contrast enhancement, Least Significant Bits (LSB) and Most Significant Bits (MSB) replacement, to name a few. On the other hand, in the frequency domain, coefficients are commonly utilized to diffuse the watermark across the host image. Recently, in Singh et al.'s method [3], lifting wavelet (LWT) and discrete cosine (DCT) transformations are applied to embed watermark. Specifically, the LH and HL subbands of LWT are utilized to embed the DCT coefficients of the transformed watermark. Later, Thakur et al. [4] put forward a watermarking method by using DWT and Singular Value decomposition (SVD) [5]–[8] and a logistic map to further enhance the robustness. Furthermore, watermark is embedded in the diagonal of 2D singular vector. Watermarking methods based on hyper-chaotic encryption [9] and Logistic Sine Coupling Map pixel shuffling [10] are also proposed, where higher robustness is achieved. Moreover, Darwish et al. [11] proposed a genetic algorithm based watermarking method by using DWT-WHT-SVD in the YCbCr color space to embed two watermarks into a host image, where WHT refers to Walsh Hadamard Transform. The two watermarks are used in tandem to achieve high payload and imperceptibility. In [12], tensor mode expansion (TME) based image watermarking method is proposed and the watermark is embedded in the DCT transformed SVD singular matrix. In addition to TME, in [7], DCT-DWT and Discrete Fractional Random Transform (DFRN) transform and Arnold [13], [14] and logistic maps based image watermarking scheme is proposed. DCT is then applied on each 8×8 block of the LL subband to generate feature vectors and the watermark is embedded in the medium frequency coefficients of DFRN.

While improvements are achieved in the aforementioned methods, there are still various drawbacks to be addressed. For example, tampered data recovery is not handled by [1-10]. Furthermore, in [3], MD5 is utilized to encrypt the watermark, which is vulnerable in nature. Moreover, SVD [8] is also vulnerable to channel attack, which has been pointed out in [15]. Although SVD provides good imperceptibility feature, it does not offer high robustness and high payload [16], because only the diagonal components are manipulated to embed watermark.

Motivated by the aforementioned drawbacks, this paper puts forward a robust high payload image watermarking method based on Arnold mapping (encryption) and multi interpolated transformations. Specifically, a watermark is embedded into an encrypted host image, which subsequently diffuses the watermark throughout the host image when it is inversely mapped to the spatial domain, essentially achieving the non-Newtonian effect (NNE) in fluid dynamics [17]. In addition, watermark is embedded into the DWT coefficients of the encrypted image, while the resulting DWT coefficients are inversely transformed by using inverse singular wavelet transformation (iSWT). This DWT-iSWT pipeline adds another layer of complication for an attacker to extract as well as to

alter the embedded watermark. Experiments are carried out to verify the performance of proposed method and to compare it against the current state-of-the-art (SOTA) methods. Our paper makes the following contributions: (a) adapting fluid dynamics non-Newtonian effect in developing image watermarking method, (b) exploiting non-Newtonian effect and SWT-DWT to achieve high robustness against channel attacks as well as compression, (c) producing high quality watermarked image despite using all host channels in the image to carry the watermarks, and (d) allowing watermark of multiple sizes to be embedding into different channels, hence providing flexibility to the proposed method.

II. Proposed Method

This section details the novel NNE of Arnold mapping and image watermarking using interpolated DWT-iSWT. NNE is a key theory in fluid dynamics, which relates fluid viscosity, pressure, and resistance [17]. Specifically, the fluid becomes more resistant when more pressure is applied upon it, following the relationship $R \propto P$, where $P \in \{1, 2, 3, ...\}$ is the pressure and $R \in [0, 1]$ is the resistance. Therefore, the higher the viscosity V, the less the resistance R, and vice versa. In other words, $V/R = \frac{1}{P}$. Specifically, $R = 1$ implies that an effective viscosity point is achieved. Hence, $R_{max} = \lim_{x\to 0} R(x)$ is the maximum R value. In this work, we apply this concept by treating our watermark being a pressure *applied* onto the host image. In addition, the pipeline of DWT-iSWT is put forward to produce a watermarked image.

A. Watermark embedding process

Our design aims at diffusing the watermark throughout the image so that it is robust against attacks. Essentially, when we embed watermark into a securely encrypted image, the embedded watermark will be diffused throughout the image (viz., absorbed by the image) when it is decrypted to produce the (plaintext) watermarked image. The steps below are applied to embed watermark into the host image H.

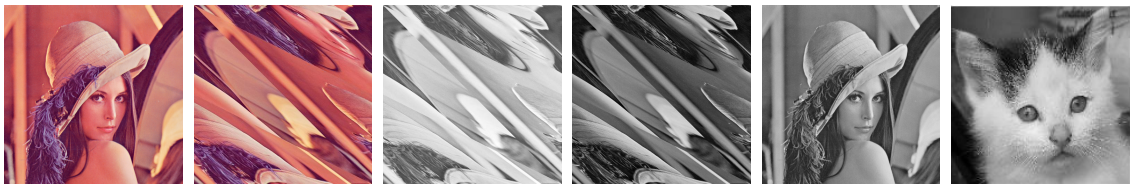
1) H is encrypted (to obtain H_e) by using the k-level Arnold chaotic map, i.e., $P' = (A^k \times P) \mod N$, for $P = [a; b; c]$, $P' = [a'; b'; c']$ and
$$A = \begin{bmatrix} 1 & c_1 & c_2 \\ c_3 & 1 + c_1c_3 & c_2c_3 \\ c_4 & c_1c_2c_3c_4 & 1 + c_2c_4 \end{bmatrix}, \quad (1)$$
where c_i's are positive numbers. This pixel value mapping function scrambles the original value P at location (x, y) to P' at location (x', y'), and k is the NNE effect handler that determines the order of the Arnold map.
2) The watermark image W is resized to half the dimensions of H and named it as W_a. The first channel (e.g., green) of H_e, denoted by H_e^1, is transformed by using 1-level DWT, i.e., $[LL_1, HL_1, LH_1, HH_1] = DWT(H_e^1)$. The LL_1 subband is modified to embed W_a as follows:
$$LL_1 \leftarrow (\alpha_1 * W_a + LL_1) + (\alpha_2 * r_1), \quad (2)$$
where r_1 is a pseudo-randomly generated sequence. α_1 and α_2 control the strength of the watermark and the randomness (noise) to be added to the output image, respectively. All subbands (i.e., LL_1, HL_1, LH_1 and HH_1) are then re-scaled to match the size of H, in preparation for later processing by using iSWT.
3) The second channel (e.g., red) H_e^2 is transformed by using a 2-level DWT and the resulting subbands are utilized as the host for the watermark W_b, which is obtained by scaling W to a quarter of the size of H. The subband LL_2 is then modified to embed W_b as follows:
$$LL_2 \leftarrow (\alpha_1 * W_b + LL_2) + (\alpha_2 * r_2), \quad (3)$$
where r_2 is a pseudo-randomly generated sequence. Here, LL_2 is the subband responsible for encoding a low resolution version of W (i.e., W_b) as a backup, in case of data loss or tampering while $r_1 \neq r_2$.
4) After the embedding process, the first host channel $H_{e,w}^1$ is inversely transformed to the spatial domain by using iSWT on the processed LL_1, HL_1, LH_1, and HH_1 subbands, causing the embedded watermark to be diffused throughout the image in the spatial domain. The second channel $H_{e,w}^2$ is transformed by using a 2-level iDWT.
5) For quick verification or tamper detection purposes, a 3D-Arnold encrypted watermark W_c is embedded in the third channel (e.g., blue) H_e^3 as follows:
$$H_{e,w}^3 \leftarrow (H_e^3 + W_c * (\alpha_1 + \alpha_2)/2) + (r'_{1^2} + r'_{2^2})/2, \quad (4)$$
where r'_1 and r'_2 are the up-scaled 2D randomization vectors.
6) Inverse Arnold mapping (decryption) is applied to the modified channels to obtain the watermarked image H_w.

Figure 1 shows the intermediate image for various stages. It is noteworthy that the proposed solution is non-fragile in nature. It is capable of resisting channel attacks and maintaining the backup watermark image in the host image, which is put in place for data preservation or recovery in case of tampering or data loss.

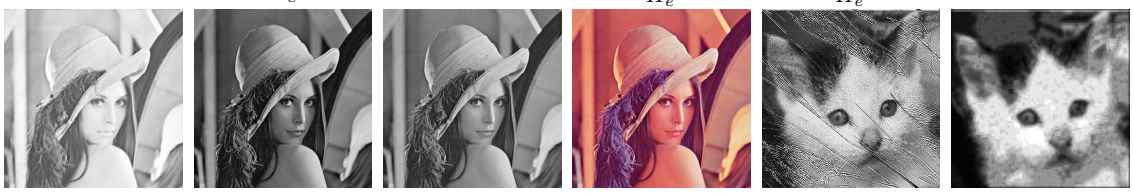
B. Watermark extraction process

Here, the extraction of watermark from a watermarked image H_w, which could have undergone some attacks, is detailed. Essentially, it is the reverse of the embedding process.

1) All RGB-channels are mapped by using the same k-level of Arnold map.
2) SWT is first applied to the first channel H_e^1, and the dimension of the resulting LL subband is halved. The embedded watermark W_a is extracted by using
$$W_{a,x} = \frac{LL(H_{e,w}^1) - (\alpha_2 * r_1) - LL(H_e^1)}{\alpha_1}, \quad (5)$$
where the original host image H is required.
3) Similarly, 2-level DWT is applied on $H_{e,w}^2$ and H_e^2, viz., DWT(DWT($H_{e,w}^2$)) and DWT(DWT(H_e^2)). The LL_2



(a) Host Image, H (b) Encrypted host, H_e (c) 1st Channel, H_e^1 (d) 2nd Channel, H_e^2 (e) 3rd Channel, H_e^3 (f) Watermark, w



(g) Watermarked, $H_{e,w}^1$ (h) Watermarked, $H_{e,w}^2$ (i) Watermarked, $H_{e,w}^3$ (j) Watermarked, H_w (k) Extracted, W_x (l) Extracted, W_x^b

Fig. 1: Intermediate images produced by proposed image watermarking method. Here, (b) is produced by using $k = 2$.

(a) F-16 Jet (b) Barbara (c) Pepper

Fig. 2: Additional host images for experiments.

subband from both $H_{e,w}^2$ and H_e^2 are utilized to extract the backup watermark W_b:

$$W_{b,x} = \frac{LL_2(H_{e,w}^2) - (\alpha_2 * r_2) - LL_2(H_e^2)}{\alpha_1} \quad (6)$$

Subsequently, the extracted watermarks $W_{b,x}$ and W are compared to quantify the data loss as well as for recovery purposes.

4) Finally, the 3D-Arnold encrypted watermark W_c is extracted for quick verification purposes by using

$$W_{c,x} = \frac{(H_{e,w}^3 - (r_1^2 + r_2^2)/2 - H_e^3)}{(\alpha_1 + \alpha_2)/2}. \quad (7)$$

III. Experiments

The proposed method is implemented in Matlab 2020 running on a Windows 10 platform with Core i7-7th Gen 7500u and 16GB of memory. The standard test images shown in Fig. 1 (i.e., Lenna), Fig. 2 (i.e., F-16 jet, Barbara, and Pepper), as well as the MSRA dataset (10K images) are considered for empirical experiments and comparison with SOTA methods. For simplicity, the Haar wavelet is adopted. Here, we set $\alpha_1 = 0.02$ and $\alpha_2 = 0.03$. The cat image shown in Fig. 1(e) is utilized as the watermark for experiment purposes and it is a quarter of the size of the host image. Results confirm that the

TABLE I: Experiment results after embedding watermark.

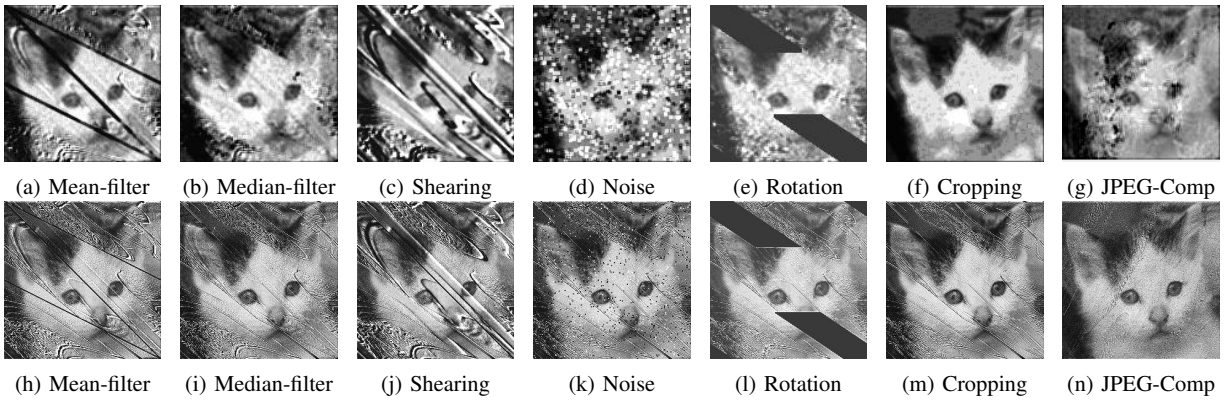
Image	Proposed	[9]	[10]	[11]	[13]	[8]
	Lenna					
PSNR (dB)	**48.59**	31.00	39.97	31.43	40.22	44.04
SSIM	**0.9992**	-	0.9874	-	-	0.9740
μ for W_b	0.9838	0.9864	**1**	0.4425	0.9820	0.9761
	F-16 Jet					
PSNR (dB)	**47.89**	32.33	39.30	31.46	40.20	44.04
SSIM	**0.9999**	-	0.9867	-	-	0.9740
μ for W_b	0.9980	0.9807	**1**	0.4931	0.9630	0.9761
	Barbara					
PSNR (dB)	**48.11**	31.78	42.11	37.99	40.32	44.04
SSIM	**0.9993**	-	0.9933	-	-	0.9740
μ for W_b	**0.9915**	0.9769	0.9908	33.97	0.9750	0.9761
	Pepper					
PSNR (dB)	**48.09**	33.78	39.30	40.08	40.05	44.04
SSIM	**0.9999**	-	0.9867	-	-	0.9740
μ for W_b	**0.9871**	0.9862	0.9827	0.4263	0.9700	0.9761

embedded watermarks, i.e., W_a, W_b, and W_c, can be extracted from the watermarked image.

To examine the visual quality of the watermarked image, the respective color channels of the original H and watermarked images H_w are compared in terms of PSNR and SSIM. Note that each value presented is the average of all three RGB-channels. Table I records the results for the proposed method and [9]–[11]. It is observed that the proposed method produces watermarked images with PSNR $>$ 47.89dB and SSIM $>$ 0.9992. These results suggest a high similarity between the original host and watermarked images. Similarly, the normalized correlation (NC), denoted by $\mu(W_k, W_{k,x})$, between the original and extracted watermark is also high, i.e., $\mu > 0.9838$. Here, $k \in \{1, 2, 3\}$ and μ is computed as

$$\mu = \frac{(w - \mu_w)(w' - \mu_{w'})}{\sqrt{(w - \mu_w)^2}\sqrt{(w' - \mu_{w'})^2}}, \quad (8)$$

where μ_w and $\mu_{w'}$ are the mean value of the original and extracted watermarks. Note that $\mu \in [0, 1]$, where larger value implies high correlation, and vice versa. Next, the



(a) Mean-filter (b) Median-filter (c) Shearing (d) Noise (e) Rotation (f) Cropping (g) JPEG-Comp

(h) Mean-filter (i) Median-filter (j) Shearing (k) Noise (l) Rotation (m) Cropping (n) JPEG-Comp

Fig. 3: Extracted watermarks (1st row for W_a, 2nd row for W_b) from the attacked watermark Lenna image H'_W.

TABLE II: Results μ after applying watermark attack.

Attack	w_a	w_b	[9]	[10]	[11]	[13]	[8]
Mean-filter	0.9447	0.9545	**0.9864**	0.9363	0.9338	-	0.9454
Median-filter	0.9648	0.9780	**0.9911**	-	-	0.9540	-
Shearing	0.9064	**0.9375**	-	-	-	-	-
Noise	0.9449	0.9588	0.8565	0.9431	**0.9900**	0.9910	0.9134
Rotation	0.9465	**0.9543**	0.8989	0.9045	0.6323	0.9490	0.8755
Cropping	0.9793	**0.9838**	-	0.9438	0.9509	0.9660	0.9653
JPEG-Comp	0.9793	**0.9838**	-	0.9438	0.9509	0.9760	0.8470

following six attacks are applied on the watermarked image, namely, mean-filter, median-filter, affine shearing with $[100; 0.510; 001]$, additive noise (0.05), rotation of 45^o, and cropping with dimension $[75 : 424; 68 : 424]$. The extracted watermarks are shown in Fig 3. As expected, each attack leads to different distortion pattern, but in general, the extract watermark is still perceivable. Crucially, the watermark is able to survive each attack with $\mu > 0.9$, and the result for each attack is recorded in Table II (see 2nd column). The performance for the backup watermark W_b is also evaluated. We compute $\mu(W_b, W_{b,x})$ by using Eq. (8), and the results are recorded in Table I (see 3rd column). Results suggest that the quality of the backup watermark W_b is also well maintained for all applied attacks with $\mu > 0.9375$. This outcome also agrees with the quality of the extracted backup watermark $W_{b,x}$ as shown in Fig. 3. It is noteworthy that the NC value of the backup watermark W_b is higher than that of the watermark W_a, although W_a is $\times 4$ the size of W_b. A reason for this outcome is that W_b is embedded into the coefficients in the 2-level of DWT, while W_a is embedded into the coefficients in the 1-level of DWT. Based on the outcome presented above, we conclude that the proposed watermarking method is robust against common watermark attacks.

Next, we compare our work with the state of the art methods. Specifically, we consider the work by Kang et al. [9], Prabha et al. [10], Darwish et al. [11], Wu et al. [8], and Pouhadi et al. [13]. Here, the same amount of watermark information is embedded into the host image, and the same attacks are applied. The results are summarized in Table I (see column 3-7) before applying any attacks and in Table II (see column 4-8) after applying different attacks. It is observed that our proposed NNE watermarking method outperforms SOTA methods in terms of image quality for both PSNR and SSIM, although the NC value is lower than Prabha et al.'s method [11] by a small margin under the no-attack scenario. When the same attacks are applied, mixed results are observed. Although the proposed method does not exhibit the highest NC scores for some attacks (e.g., mean-filter, noise), the performance is only slightly inferior to the best method (e.g., for mean-filter, we are only 3% lower). All in all, the proposed method achieves a well-balanced performance in comparison to [9]–[11], and it produces watermarked images with the highest quality. Furthermore, the state of the art methods hide less payload (i.e., without a backup image), while the proposed method hides extra watermarks, i.e., W_b and W_C for tamper detection and recovery purposes. Moreover, our work is the first to combine the concepts of SWT-DWT and NNE Arnold domain for watermarking purposes, which is shown here to offer high robustness and image quality.

IV. Conclusion

In this work, the concept of Non-Newtonian effect in fluid dynamics is adapted to put forward an image watermarking method. Specifically, the host image is encrypted by using Arnold mapping and the watermark is embedded into the encrypted host so that the watermark is diffused throughout the host image when it is decrypted to produce the plaintext watermarked image. Results confirmed that proposed watermarking scheme is robust against common channel attacks, and it outperforms the conventional methods in terms of image quality.

As future work, our aim is to analyze other watermark diffusion techniques to further enhance robustness and embedding capacity. In addition, more extensive experiments will be conducted and reported.

Acknowledgment

This work is supported by Advanced Engineering Platform's Cluster Funding (account number AEP-2021-Cluster-04), Monash University Malaysia.

REFERENCES

[1] Q. Li, B. Yan, H. Li, and N. Chen, "Separable reversible data hiding in encrypted images with improved security and capacity," *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 30 749–30 768, 2018.

[2] 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.

[3] A. K. Singh, "Robust and distortion control dual watermarking in lwt domain using dct and error correction code for color medical image," *Multimedia Tools and Applications*, vol. 78, no. 21, pp. 30 523–30 533, 2019.

[4] S. Thakur, A. K. Singh, S. P. Ghrera, and A. Mohan, "Chaotic based secure watermarking approach for medical images," *Multimedia Tools and Applications*, vol. 79, no. 7, pp. 4263–4276, 2020.

[5] S. B. B. Ahmadi, G. Zhang, and S. Wei, "Robust and hybrid svd-based image watermarking schemes," *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 1075–1117, 2020.

[6] E. Najafi and K. Loukhaoukha, "Hybrid secure and robust image watermarking scheme based on svd and sharp frequency localized contourlet transform," *Journal of information security and applications*, vol. 44, pp. 144–156, 2019.

[7] N. R. Zhou, W. M. X. Hou, R. H. Wen, and W. P. Zou, "Imperceptible digital watermarking scheme in multiple transform domains," *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 30 251–30 267, 2018.

[8] J.-Y. Wu, W.-L. Huang, W.-M. Xia-Hou, W.-P. Zou, and L.-H. Gong, "Imperceptible digital watermarking scheme combining 4-level discrete wavelet transform with singular value decomposition," *Multimedia Tools and Applications*, vol. 79, pp. 22 727–22 747, 2020.

[9] X.-b. Kang, G.-f. Lin, Y.-j. Chen, F. Zhao, E.-h. Zhang, and C.-n. Jing, "Robust and secure zero-watermarking algorithm for color images based on majority voting pattern and hyper-chaotic encryption," *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 1169–1202, 2020.

[10] K. Prabha and I. S. Sam, "A novel blind color image watermarking based on walsh hadamard transform," *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 6845–6869, 2020.

[11] S. M. Darwish and L. D. S. Al-Khafaji, "Dual watermarking for color images: A new image copyright protection model based on the fusion of successive and segmented watermarking," *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 6503–6530, 2020.

[12] F. Jiang, T. Gao *et al.*, "A robust zero-watermarking algorithm for color image based on tensor mode expansion," *Multimedia Tools and Applications*, pp. 1–16, 2020.

[13] A. Pourhadi and H. Mahdavi-Nasab, "A robust digital image watermarking scheme based on bat algorithm optimization and surf detector in swt domain," *Multimedia Tools and Applications*, pp. 1–25, 2020.

[14] K. Li, Y. Soh, and Z. Li, "Chaotic cryptosystem with high sensitivity to parameter mismatch," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, no. 4, pp. 579–583, 2003.

[15] H.-C. Ling, R. C.-W. Phan, and S.-H. Heng, "Attacks on svd-based watermarking schemes," in *International Conference on Intelligence and Security Informatics*. Springer, 2008, pp. 83–91.

[16] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Security analyses of false positive problem for the svd-based hybrid digital image watermarking techniques in the wavelet transform domain," *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 26 845–26 879, 2018.

[17] L. Yang and K. Du, "A comprehensive review on the natural, forced, and mixed convection of non-newtonian fluids (nanofluids) inside different cavities," *Journal of Thermal Analysis and Calorimetry*, pp. 1–22, 2019.