Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 2, November 2021, pp. 864~870
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i2.pp864-870

Self embedding digital watermark using hybrid method against compression attack

Nasr Eddine Touati, Abdelmounaim Moulay Lakhdar
Information Processing and Telecommunication Laboratory (LTIT), Faculty of Technology,
University TAHRI Mohammed Bechar, Bechar, Algeria

Article Info

Article history:

Received Aug 22, 2021
Revised Sep 22, 2021
Accepted Sep 27, 2021

Keywords:

Digital watermark
Hybrid
Image processing
Invisible
JPEG
LSB-watermarking
SVD

ABSTRACT

In the modern time interacting with digital world become standard life activity, human need a way to protect properties as individuals or corporals, and we do that by embedding a digital mark to the target, and this technique call digital watermarking. But there still is a chance to manipulate or even remove this marks we embed for protection with various attacks like adding noises, compression-decompression or bits manipulations, and that why companions, individuals, laboratories are still developing new methods to embed this marks and make them more robust and more hard to detect for others. There are so many methods for digital watermarking, so we chose the least significant bits watermarking (LSB-watermarking) to provide an invisible digital watermarking, and on top of that we proceed with the blind LSB-watermarking metho d so that we don't get bind to the original image, and for our attack we chose compression joint photographic experts group (JPEG) compression because it's the most used method for image and videos compression along with singular value decomposition (SVD) to make our mark as robust as possible. And the results we gain from our method are promising and it did give as high quality digital watermarking.

Corresponding Author:

Nasr Eddine Touati
Information Processing and Telecommunication Laboratory (LTIT), Faculty of Technology
University TAHRI Mohammed Bechar
Bechar, Algeria
Email: touati.nasreddine.dz@gmail.com

1. INTRODUCTION

Digital watermarking is an image process grounded on image manipulations to allows us to add some information we chose to our image with visible or invisible way and that depend on the use of that information, there two major uses for digital watermarking, first image authentication and image data hiding. The purpose of image authentication is for detecting malicious manipulation, but these old methods consider some other image manipulations as attacks like compression and image enhancement, and the purpose of image data hiding is to embed a secret information within the cover image as large as possible with minimal degradation for the cover image. Therefore, digital watermarking have two important parts for it to be consider a practical one which is invisibility without destroying the visual properties and the robustness of the digital watermark [1]-[3].

Our technique is quantization coefficients-based manner and for those requirement we are using least significant bits watermarking (LSB-watermarking) but the earlier methods requires an encryption with a key so even if they don't need the original image they're still bind to the key which they can't extract the mark if they lost it, however our technique work in smarter why which don't need the original image or an

encryption for the mark before embedding so no more need for the key and provide the least distortion on our cover image with the most secured way. Therefore, as long as we have the proper equipment and software we will be able to embed and extract the digital watermark without problem.

This quantization coefficients-based technique with the help of singular value decomposition (SVD) is for self-embedding digital watermark whenever there a joint photographic experts group (JPEG) attack (compression decompression) is applied and its will be embedded in all the LSB bits for more efficiency. And for such results we watermark the quantization coefficients with 8x8 mark, and when the quantization on the discrete cosine transform (DCT) is applied the mark will be embedded alongside it on the cover image using the coefficients, but in normal pattern way the distortions will be high because we are using the 8^{th} bit in each coefficient to create a robust digital watermark on the quantization coefficients and that will lead to major distortions all over the cover and also could lead to make the digital watermark to be visible, SVD method provide a manipulation that can help us to prevent this problem by creating a coefficients with embedded digital watermark on the 8^{th} bit for the most robustness and also as invisible as possible. To be more specific our SVD-DCT hybrid technique work as self-embedding digital watermark, by implementing it as a sleeping parameter that get activated in case of JPEG compression attack.

2. REVIEW OF RELATED WORKS

In the past years digital images watermarking developed quite dramatically, and there's so many methods and technique for that [4], [5], and its change from a domain to another medical, telecommunication, copyright registration to just simple effect for images and videos [6]-[8], but each one of them need some parameters like original image or a key to extract the digital watermark correctly [9]-[11], which mean a big problem in case lose or destroy this parameters, that will lead to incapability for the extraction [12]-[14], in other words embedding a mark in the LSB of images with simple methods alone, and not using any encryptions or other data hiding techniques is too fragile for be used alone to counter any kind of data manipulation [15], [16]. But in this paper we propose a solution for this problem, by creating a method to embed a digital watermark, and extracting it after regardless for the need for any other parameters using any standard LSB extracting method to get the watermark.

3. REQUIRED KNOWLEDGE

3.1. SVD

Singular value decomposition (SVD) is numerical analysis method used to analyze matrices with multiple application, with this technique we can decompose a matrix three matrices with the same size as the original matrix [17], [18], where the U and V components are $n \times n$ real unitary matrices with small singular values, and the S component is an $n \times n$ diagonal matrix with larger singular value entries which satisfy $S_{(1,1)} \geqslant S_{(1,2)} \geqslant S_{(1,3)} \geqslant S_{(1,4)}$ [19]. B is the reconstructed matrix after the inverse SVD transformation is applied B = $U \times S \times VT$.[19] such as for the matrix A:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \text{ and [U, S, V] = SVD (A), is:}$$

$$U = \begin{pmatrix} -0.21483724 & 0.88723069 & 0.40824829 \\ -0.52058739 & 0.24964395 & -0.81649658 \\ -0.82633754 & -0.38794278 & 0.40824829 \end{pmatrix},$$

$$S = \begin{pmatrix} 1.68481034e+01 & 0 & 0 \\ 0 & 1.06836951e+00 & 0 \\ 0 & 0 & 4.41842475e-16 \end{pmatrix},$$

$$V = \begin{pmatrix} -0.47967118 & -0.57236779 & -0.66506441 \\ -0.77669099 & -0.07568647 & 0.62531805 \\ -0.40824829 & 0.81649658 & -0.40824829 \end{pmatrix}, \text{ and B} = U \times S \times V^T$$

3.2. JPEG

JPEG method mainly consists of three steps, namely DCT, quantizer, and entropy encoder. Firstly, we apply two-dimensional DCT to the non-overlapping 8×8 blocks, this step will transformed the original image from the spatial domain to the frequency domain. Secondly the obtained DCT coefficients are then treated with the predetermined quantization coefficient and quantized. Thirdly we will coordinate the

quantized DCT coefficients with zigzag scanning order and after that run length encoding (RLE) after all this we get the compressed information, and for reconstructing the information we need to go in reverse for all the steps [12]-[21]. The two-dimensional DCT:

$$\frac{2}{\sqrt{(MN)}} C(m)C(n) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f\ (x,y) cos \frac{(2x+1)m\pi}{2M} cos \frac{(2y+1)n\pi}{2N} \quad (1)$$

where: C(m),C(n)=$1/\sqrt{2}$ for m,n=0 and C(m),C(n)=1 otherwise. The inverse two-dimensional DCT:

$$\frac{2}{\sqrt{(MN)}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} C\ (m)C(n) f(m,n) cos \frac{(2x+1)m\pi}{2M} cos \frac{(2y+1)n\pi}{2N} \quad (2)$$

where and C(m),C(n)=$1/\sqrt{2}$ for m,n=0 and C(m),C(n)=1 otherwise. F (m, n) is the DCT of the signal f(x, y)

3.2. LSB

LSB-watermarking method is used for frequent processes to embed information in a cover image, that we change the inside of a cover image pixels by bits of the secret message. We change the first bits from the cover image, with the bits of our secret message depending on the needed changes according to the embedded message. Usually only the first half of the bits of each pixel from the cover image needed to be replaced with secret message bits because it's only needed low bits for embedding the secret message. In Figure 1, and this adjustments will result in low changes in intensity of the colors but it will not be noticeable for the human eyes [2], [22], [23].

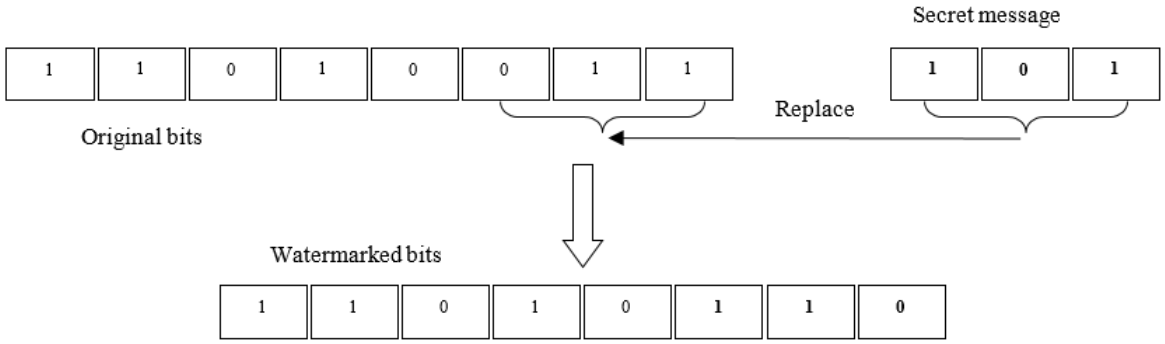

Figure 1. An example of 3rd bit LSB

4. PROPOSED METHOD

This section is for describing our technique, we are watermarking the quantization coefficients (Q) for the DCT with 8x8 image to get the Qw, then we applies the SVD on bought of the coefficients Q and Qw to get the fallowing matrix Uq, Sq, Vq from Q, and Uqw, Sqw, Vqw from Qcw. then we use the Sqw and reversed the SVD with Uq and VqT to recreate a new coefficients matrix as like shown in the (3). And this method gives us another property, that when the more the lower of the quantization quality the more robust the digital watermark and behave with self-embedding on all over the original image, and the thanks is to watermarking on the 8th bit and that why it's perfect for countering JPEG attacks.

[Uq, Sq, Vq] = SVD (Q)
[Uqw, Sqw, Vqw] = SVD (Qw) (3)
NQw = [Uqw× Sq× VqwT]

After that we continue in our compression and applied the DCT on each 8x8 block of the cover image, the digital watermark will be embedded automatically in all the 8x8 blocks of the cover, we will notice there a little different in the positioning about the watermark bits with a change on bought axes X and Y equal to (-1,-1) compared to the original after extraction. Figures 2(a) and 2(b), and that because of the DCT. And on the opposite of other techniques, we don't need any other parameters to extract the digital watermark.

(a) (b)

Figure 2. The used image for watermarking: (a) original watermark and (b) the extracted mark

4.1. Embedding process

In this section, we present our embedding method. Figure 3, a quantization coefficients-based watermarking scheme. Both the embedding procedure and extracting procedure are included. The overview of the proposed digital watermarking scheme is shown.

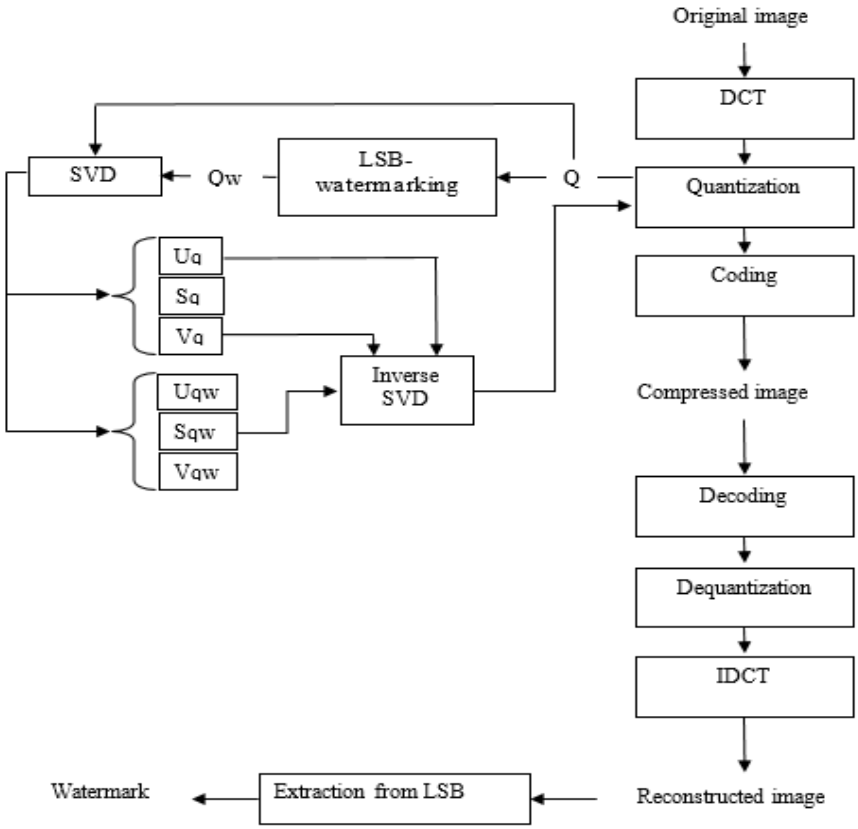

Figure 3. Diagram of quantization coefficient method

5. RESULT AND DISCUSSION

In our experimental results, a 512x512 grayscale image which is shown in Figure 4(a) were used as cover image. when, we embed the secret data which contain our watermark 'letter T', we got a watermarked image without Figures 4(b)-(f) noticeable distortion in case of higher quantization coefficient quality and the lower the quality the more the digital watermark become robust tell it overwhelm the most significant bits (MSB) values.

Figures 4(b)-(i) represent the digital watermarked images with bought standard and our method techniques with the same quantization coefficients values, and we can see the different represent in the less distortion for the proposed method. And we notice the watermark work like defense technique against JPEG attack and, where it is become more and more robust and visible each time we lower the quantization coefficients values, we notice in Figure 4(b) with Q=90, that the digital watermark on the 8^{th} bits is completely invisible and there no noticeable distortion with our method while in Figure 4(c) with Q=90 the disrotion is completely visible, and Figure 4(d) with Q=85 its similar to Figure 4(b) while using our method, while Figure 4(e) get more destored.

Meanwhile our new digital watermarking method in Figure 4(f) with Q=75 is better than the normal method in Figure 4(g) with the same Q, the, normal digital watermark dealt a great distortion on the cover image, and even more on lower quantization coefficients values, but even in lower values in Q our method still better and that is manifested in Figure 4(h) with Q=35 it's a little bit clearer then Figure 4(i) with Q=35. The quality of each good restored image is provided in Table 1.

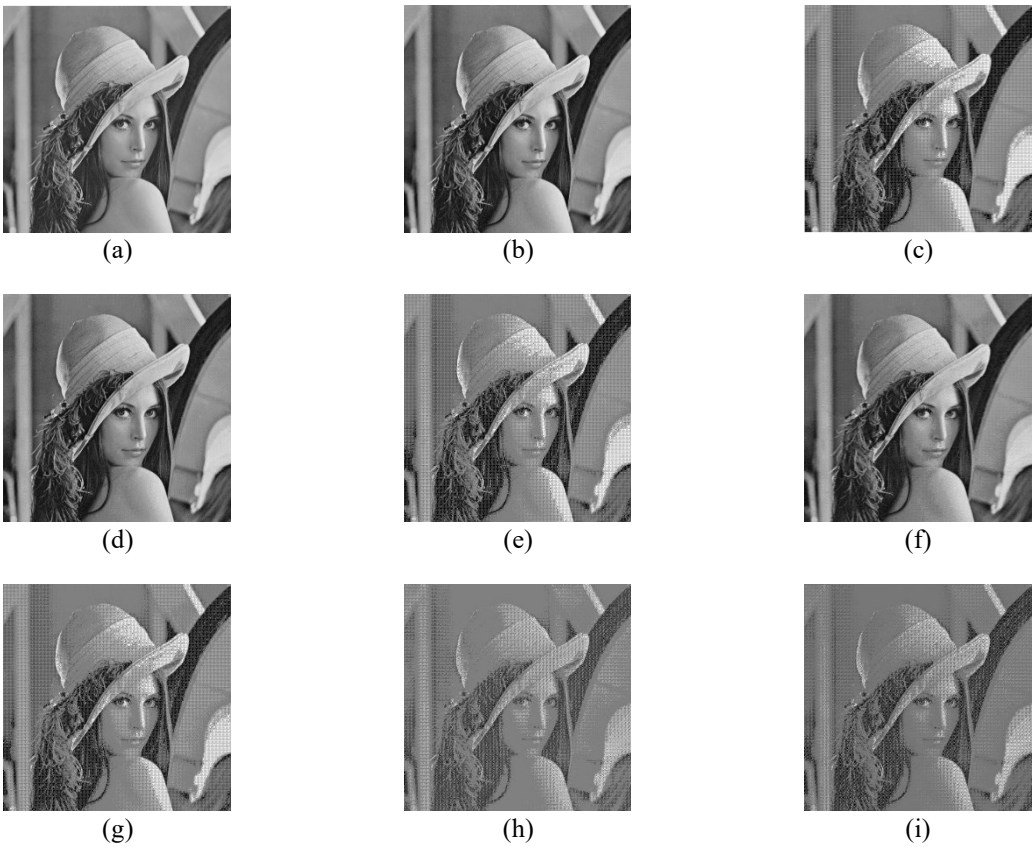

Figure 4. The original image compared to watermarked images: (a) original, (b) new watermarked Q=90, (c) normal watermarked Q=90, (d) new watermarked Q=85, (e) normal watermarked Q=85, (f) new watermarked Q=75, (g) normal watermarked Q=75, (h) new watermarked Q=35, and (i) normal watermarked Q=35

The structural similarity (SSIM) index quality assessment index is the ration of the computation of three terms, namely the contrast term, the luminance term and the structural term. The overall index is a multiplicative combination of the three terms [24].

$$SSIM(x,y) = [l(x,y)]\alpha \cdot [c(x,y)]\beta \cdot [s(x,y)]\gamma \backslash \quad (4)$$

where:

$$l(x,y) = \frac{2\mu_x\mu_y+C_1}{\mu_x^2+\mu_y^2+C_1}, \quad C(x,y) = \frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2+\sigma_y^2+C_2}, \quad S(x,y) = \frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3} \quad (5)$$

Table 1. The peak signal-to-noise ratio (PSNR) and mean structural similarity (MSSIM) value of each reconstructed image

Quantization coefficients	PSNR (dB)	MSSIM
Q = 90	33.89	0.9262
Q = 85	32.68	0.8801
Q = 80	30.81	0.8037
Q = 75	29.63	0.7326

In the extraction we obviously don't need all the digital watermarks with embed in all the cover we only need one, so we extract all the LSB from the image then we run 8x8 size contour scanner to detect the digital watermark like Figures 5(a)-(e). Like what we are noticing there is a low-quality extraction cases, but it still recognizable and for that we add a threshold to our 8x8 contour scanner to consider every case above 80% as a valid result Table 2.

(a) (b) (c) (d) (e)

Figure 5. The extracted watermark: (a) best extraction case, (b) medium extraction case, (c) medium extraction case, (d) medium extraction case, and (e) lower extraction case

Reconstructed mages are evaluated by the peak signal-to-noise ratio PSNR, it's the most commonly used as a measure of quality for images compressions, it is the most easily defined via the mean squared error (MSE) which for the two images original and the reconstructed, the PSNR value approaches infinity as the MSE approaches zero; this means higher PSNR value provides a higher image quality [25]. And the equation defined as (6) and (7);

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{ij} - g_{ij})^2 \quad (6)$$

$$\text{PSNR} = 10log_{10}(^{255^2}/_{MSE(f,g)}) \quad (7)$$

And surprisingly our method behave the same way in in transmission channels which mean lower the channel quality the stronger the robustness of our mark.

Table 2. Threshold and PSNR of the extracted watermark

Extracted mark	Threshold calculated	PSNR (dB)
a	100%	30.03 (Accepted mark)
b	93.3%	29.11 (Accepted mark)
c	94.1%	28.94 (Accepted mark)
d	71.22%	27.56 (Rejected mark)

6. CONCLUSION

this paper propose a new hybrid digital image watermarking method based on quantization coefficient and singular value decomposition SVD, which helps us to embed a digital watermark in the 8th bit of cover image without distorting the cover and still invisible, also having a defensive behavior against JPEG attack that the digital watermark become more robust and more aggressive tell the digital watermark change the position from the LSB to the most significant bits (MSB) in all the pixels of the cover and become more visible to human eyes in case of big attacks. And in addition it's behave the same with channel noises surprisingly, and for more efficient result we are looking to add a machine learning section to obtain the changing patterns of the attacks to predict futures attacks, and prepare a more efficient way to counter them.

ACKNOWLEDGEMENTS

This work is supported by Information Processing and Telecommunication Laboratory (LTIT).

REFERENCES

[1] S. D. Lin, S. C. Shie, and J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," *Computer Standards & Interfaces*, vol. 32, no. 1-2, pp. 54-60, Jun. 2010, doi: 10.1016/j.csi.2009.06.004.

[2] G. K. Wallace, "The JPEG still picture compression standard," *IEEE Transactions on Consumer Electronics*, vol. 38, no. 1, pp. xviii – xxxiv, Feb. 1992, doi: 10.1109/30.125072.
[3] N. Alias and Ferda Ernawan, "Multiple watermarking technique using optimal threshold," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 1, pp. 368-376, Apr. 2020, doi: 10.11591/ijeecs.v18.i1.pp368-376.
[4] A. Mohanarathinam, S. Kamalraj, G. K. D. P. Venkatesan, R. V. Ravi, and C. S. Manikandababu, "Digital watermarking techniques for image security: a review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 3231-3229, Sep. 2019, doi: 10.1007/s12652-019-01500-1.
[5] S. Haddad, G. Coatrieux, A. M. Gaudry, and Michel Cozic, "Joint Watermarking-Encryption-JPEG-LS for Medical Image Reliability Control in Encrypted and Compressed Domains," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2556-2569, Feb. 2020, doi: 10.1109/TIFS.2020.2972159.
[6] A. Nagm and M. Safy, "A Robust Watermarking Algorithm for Medical Images," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 14, no. 2, pp. 01-14, May. 2019, doi: 10.11591/ijeecs.v14.i2.ppab-cd.
[7] F. Q. A. Al-Yousuf and R. Din, "Review on secured data capabilities of cryptography, steganography, and watermarking domain," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 2, pp. 1053-1059, Feb. 2020, doi: 10.11591/ijeecs.v17.i2.pp1053-1059.
[8] A. M. Abdulazeez, D. M. Hajy, D. Q. Zeebaree, and D. A. Zebari, "Robust watermarking scheme based LWT and SVD using artificial bee colony optimization," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 2, pp. 1218-1229, Feb. 2021, doi: 10.11591/ijeecs.v21.i2.pp1218-1229.
[9] S. Gull, N. A. Loan, S. A. Parah, J. A. Sheikh, and G. M. Bhat, "An efficient watermarking technique for tamper detection and localization of medical images," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1799-1808, Dec. 2018, doi: 10.1007/s12652-018-1158-8.
[10] S. N. Prajwalasimha, C. Suputhra, and C. S. Mohan, "Performance analysis of DCT and successive division based digital image watermarking scheme," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 2, pp. 750-757, Aug. 2019, doi: 10.11591/ijeecs.v15.i2.pp750-757.
[11] A. Bamatraf, R. Ibrahim, and M. N. B. M. Salleh, "Digital Watermarking Algorithm Using LSB," *2010 International Conference on Computer Applications and Industrial Electronics*, Jan. 2011, pp. 155-159, doi: 10.1109/ICCAIE.2010.5735066.
[12] C. C. Chang, P. Tsai, and C. C. Lin, "SVD-based digital image watermarking scheme," *Pattern Recognition Letters*, vol. 26, pp. 1577-1586, Jul. 2005, doi: 10.1016/j.patrec.2005.01.004.
[13] R. Aarthi, V. Jagayna, and S. Poonkuntran, "Modified LSB Watermarking for Image Authentication," *International Journal of Computer & Communication Technology*, vol. 6, pp. 5-8, Jun. 2015, doi: 10.47893/IJCCT.2015.1264.
[14] K. Kurihara, M. Kikuch, S. Imaizummi, S. Shiota, and H. Kiya, "An Encryption then Compression System for JPEG/Motion JPEG Standard," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E98.A, no. 11, pp. 2238-2245, Nov. 2015, doi: 10.1587/transfun.E98.A.2238.
[15] J. M. Garcia, B. P. G. Salgado, V. Ponomaryov, R. R. Reyes, S. Sadovnychiy, and C. C. Ramos, "An effective fragile watermarking scheme for color image tampering detection and self-recovery," *Signal Processing: Image Communication*, vol. 81, 2020, doi: 10.1016/j.image.2019.115725.
[16] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions," *IEEE Access*, vol. 8, pp. 166589-166611, 2020, doi: 10.1109/ACCESS.2020.3022779.
[17] R. Liu and T. Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful," *IEEE Transactions on Multimedia*, vol. 4, no, pp. 121-128, Mar. 2002, doi: 10.1109/6046.985560.
[18] J. F. Yang and C. L. Lu, "Combined techniques of singular value decomposition and vector quantization for image coding," *IEEE Transactions on Image Processing*, vol. 4, no. 8, pp. 1141-1146, Aug. 1995, doi: 10.1109/83.403419.
[19] X. Tong *et al*., "Image Registration With Fourier-Based Image Correlation: A Comprehensive Review of Developments and Applications," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 12, no. 10, pp. 4062-4081, Oct. 2019, doi: 10.1109/JSTARS.2019.2937690.
[20] A. Dapena and S. Ahalt, "A Hybrid DCT-SVD Image-Coding Algorithm," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 12, no. 2, pp. 114-121, Feb. 2002, doi: 10.1109/76.988658.
[21] F. Huang, X. Qu, H. J. Kim, and J. Huang, "Reversible Data Hiding in JPEG Images," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 26, no. 9, pp. 1610-1621, Sep. 2016, doi: 10.1109/TCSVT.2015.2473235.
[22] R. K. Singh, D. K. Shaw, and M. J. Alam, "Experimental Studies of LSB Watermarking with Different Noise," *Procedia Computer Science*, vol. 54, pp. 612-620, 2015, doi: 10.1016/j.procs.2015.06.071.
[23] G. J. Lee, E. J. Yoon, and K. Y. Yoo, "A new LSB based Digital Watermarking Scheme with Random Mapping Function," *2008 International Symposium on Ubiquitous Multimedia Computing,* Oct. 2008, pp. 130-134, doi: 10.1109/UMC.2008.33.
[24] T. Richter, "SSIM as Global Quality Metric: A Differential Geometry View," *2011 Third International Workshop on Quality of Multimedia Experience*, Nov. 2011, pp. 189-194, doi: 10.1109/QoMEX.2011.6065701.
[25] A. Horé and D. Ziou, "Image quality metrics: PSNR vs. SSIM," *2010 20th International Conference on Pattern Recognition*, Oct. 2010, pp. 2366-2369, doi: 10.1109/ICPR.2010.579.