ANALYSIS

17(47), 2020

ISSN 2319–7757
EISSN 2319–7765

Indian Journal of Engineering

A Robust Digital Image watermarking algorithm based on IWT-SVD

Saqib Ali Nawaz[1,2], Uzair Aslam Bhatti[3]✉, Raza Muhammad Ahmad[1,2], Muhammad Usman Shoukat[4], Anum Mehmood[5]

[1]College of Information Science and Technology, Hainan University, Haikou, China 570228
[2]State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou 570228, China Haikou, Hainan province, China
[3]Nanjing Normal University, Nanjing Xianlin Campus, Nanjing, Jiangsu, China
[4]School of Automation and Information Sichuan University of Science and Engineering, Yibin 644000, china
[5]Dept of Biochemistry and Molecular Biology, Hainan University, Haikou, China

Saqib Ali Nawaz - Email: saqibsial20@gmail.com
Uzair Aslam Bhatti - Email: uzairaslambhatti@hotmail.com
Raza Muhammad Ahmad - Email: wenbo1147@yahoo.com
Muhammad Usman Shoukat - Email: usmanryk12@gmail.com
Anum Mehmood - Email: gooddranam@yahoo.com

✉**Corresponding author**
Nanjing Normal University, Nanjing Xianlin Campus, Nanjing, Jiangsu,
China
Email: uzairaslambhatti@hotmail.com

Article History
Received: 23 October 2019
Accepted: 17 December 2019
Published: January 2020

Citation

Saqib Ali Nawaz, Uzair Aslam Bhatti, Raza Muhammad Ahmad, Muhammad Usman Shoukat, Anum Mehmood. A Robust Digital Image watermarking algorithm based on IWT-SVD. *Indian Journal of Engineering*, 2020, 17(47), 110-116

General Note

Article is recommended to print as color digital version in recycled paper.

ABSTRACT

In order to solve the problem of high false positive rate of traditional SVD domain digital watermarking algorithm, a digital watermarking algorithm based on IWT and SVD is proposed. The algorithm firstly decomposes the carrier image into 1 IWT to obtain 4 subbands, then performs SVD transformation on the 4 subbands, and directly embeds the watermark image information into the singular values of the 4 subbands of the carrier image. In the process of embedding watermark, a digital signature authentication mechanism is proposed. The generated digital signature is used to encrypt the watermark image by embedding a digital signature when the watermark is embedded. Before extracting the watermark, verify the digital signature to avoid false positives. Experiments show that the algorithm has good visibility and ability to resist various attacks.

Keywords: integer wavelet transform; singular value decomposition; digital signature; watermark; false alarm

1. INTRODUCTION

Integer wavelet transform (IWT) is the core part of the new generation image compression standard JPEG2000. Its main advantage is that it can realize integer-to-integer mapping in image decomposition and reconstruction process, ensuring that the image loses 0 in the transform part. A true lossless reversible wavelet transformIWT runs faster than DWT [1]. IWT is widely used in watermark encryption of digital images to protect copyright [2-3].

Singular value decomposition (SVD) is a linear algebra tool commonly used in image compression, signal-to-noise separation and so on. In [4], a self-embedding technique is proposed to propose a DWT-SVD domain full-blind robust quantization watermarking algorithm. The self-embedding feature watermark sequence and the blind extraction authentication watermark sequence are used to achieve full blind detection. In [5], an image authentication watermarking algorithm based on SVD and a pseudo-random cyclic chain composed of Logistic chaotic system is proposed, which improves thewatermark security and effectively resists vector quantization attacks. In [6], the advantages of Contourlet transform and singular value are combined. A robust watermarking algorithm based on singular value decomposition in Contourlet domain is proposed, which is robust to both conventional attacks and geometric attacks. In [7] order to improve the stability of watermark, a digital image watermark creation algorithm based on chaos and SVD-DWT is proposed. Digital image watermarks sensitive to signal processing and geometric distortion are recommended. It can show from the existing research literature that SVD combined with other analysis tools usually has good visual and robustness in digital image watermarking applications. However, the classic SVD algorithm has a high false alarm problem when extracting watermarks. Literature [8] analyzed that the root cause of the high false alarm rate of the SVD watermarking algorithm is that the base space of the image SVD decomposition is related to the image content. There is no one-to-one correspondence between the singular value vector and the image, and the geometry of the image cannot be characterized. The main defect of the algorithm is not in the extraction process, but in the embedded algorithm that only the singular value vector of the watermark image is implanted, and there is no structural information of the watermark image in the base space. Therefore, this paper proposes an improved algorithm based on block SVD and DCT decomposition. In [9] and [10], the problem of excessive false alarm probability for a class of SVD domain image watermarking schemes is proposed. An improved hybrid DWT and SVD image reference watermarking algorithm is proposed. The above improved algorithm idea is to avoid using the matrix U, V when extracting. However, once the attacker has mastered the U and V matrices of the copyright image, the unauthorized image can also be pseudo-claimed.

According to the reason that the false alarm rate of the SVD watermarking algorithm analyzed by the literature [8] is too high, the SVD transform is performed after the IWT decomposition of the carrier image, and the U and V matrix in the SVD transform is proposed in the watermark embedding process. The digital signature encryption authentication mechanism overcomes the problem of excessive false alarm of the traditional SVD algorithm, and verifies the visual and robustness of the algorithm through experiments.

2. WATERMARKING ALGORITHM OF IWT-SVD

Digital signature authentication mechanism

It has been shown that the drawback of the high false alarm rate of the SVD algorithm is that the watermark embedding uses only the singular value feature vector vector S of the carrier image, while the matrices U and V preserve most of the information of the image. If the U and V orthogonal matrices are used in extracting the watermark, A vector of singular values of the image without watermark is synthesized, and an image very similar to the original structure of the watermark image can be reconstructed, which will result in an erroneous alarm. Therefore, in this paper, we propose a signature authentication mechanism for matrices U and V to solve this problem. The authentication mechanism is divided into three parts: signature generation, signature implementation, signature extraction and verification. First, use a signature injection program to create a unique signature that is embedded in the image. In this task, the signature embedding program and the watermark embedding program are completed simultaneously. The signature is generated at the stage of embedding the watermark, and in the final stage of embedding the watermark, the signature is embedded in the image of the watermark. In the detection phase, the decoder first extracts the signature and compares it with the signature generated by the matrices U and V received by the client. If the signatures match, the authorization is granted and the watermark continues to be extracted. Otherwise, the extraction operation will end.

After the signature is generated, the image is decomposed by SVD, and the unique binary data is generated as a digital signature by the encryption algorithm to encrypt the image matrices U and V. This signature does not randomly allow an attacker to make a prediction. To improve security, a key pair algorithm is also used in the signature generation process. The digital signature process is as follows:

(a)Transforming the two-dimensional orthogonal matrix U, V after SVD decomposition into a one-dimensional array;

(b)Hashing the orthogonal matrices U, V using the SHA-1 algorithm:

$\mathrm{Dig}_{\mathrm{U}} = Hashing_{(SHA-1)}(U)$,

$\mathrm{Dig}_{\mathrm{V}} = Hashing_{(SHA-1)}(V)$.

(c) Convert Dig_U and Dig_V to the corresponding binary numbers, then XOR them, and save the result to K1.

$\mathrm{k1} = \mathrm{convert}_2\,(Dig\_{U}) \oplus \mathrm{convert}_2\,(Dig\_{V})$.

(d) Set an initial key, name it K2, convert it to a binary number, and perform an exclusive OR operation with K1, and save the result to K3.

$$\mathrm{K3} = \mathrm{K1} \oplus \mathrm{K2}$$

(e) Select the first 8 bits of the binary number K3 as the digital signature and name it Sig.

The embedded signature is performed after the watermark is embedded in the carrier image. Since the generated digital signature has only an 8-bit binary number, embedding the signature in the water-imprinted image does not affect the quality of the image. In order to achieve better robustness, the image is subjected to a 1-level DWT decomposition, and the corresponding sub-blocks of the energy-concentration sub-band LL are selected for SVD decomposition, and then the first column element of the U matrix of each sub-band is changed by changing the water-imprinted image. Embed digital signatures. Experiments have shown that it is best to embed digital signatures using the second element of the first column of the orthogonal vector of matrix U. The signature embedding process is as follows:

(a) Perform a 1-level DWT decomposition on the water-imprinted image to obtain a low-frequency sub-band LL, and divide the LL sub-band into 8*8 sub-blocks;

(b) Randomly selecting 8 sub-blocks using a key and performing SVD on each sub-block of the selected 8 sub-blocks;

(c) Select the second element of the first column of the orthogonal vector of each sub-block matrix U (ie, the second row and the first column) by 10, and then perform the rounding down.

$$U_{2,1} = [U_{2,1} \times 10]$$

(d) If the bit value of the digital signature is 1 and $U_{2,1}$is an even number, or if the bit value of the digital signature is 0 and $U_{2,1}$is an odd number, then:

$$U_{2,1} = \left[U_{2,1} + 1\right]\mathrm{mod}\ 10;$$

(e) Performing an inverse SVD operation on the selected 8 sub-blocks;

(f) The inverse DWT operation completes the embedding of the signature.

Signature extractor

(a) After performing a first-level DWT transformation on the received image, dividing the LL sub-band into 8*8 sub-blocks;

(b) Selecting a corresponding sub-block according to the set key;

(c) Performing SVD conversion on the selected sub-block;

(d) Test $U_{2,1}$ using the following formula:

$$S^{\prime}(\mathrm{i}) = \begin{cases} 1, & if\left(\left[U_{2,1} \div 10\right]\right) mod2 = 0 \\ 0, & if\left(\left[U_{2,1} \div 10\right]\right) mod2 \neq 0 \end{cases}, i = 1,2, \dots\dots..8$$

Watermark embedding

Integer wavelet transform is a typical representative of lifting wavelet transform. All classical wavelet algorithms can be implemented using the lifting wavelet algorithm, and have the advantages of high speed, no need for auxiliary memory, easy implementation and easy implementation of inverse transform [11] [12]. The integer wavelet transform is divided into three steps: splitting, prediction, and updating. In this paper, the carrier image is decomposed by integer wavelet transform, then SVD transform is performed, then the watermark image information is embedded into the singular value of the carrier image by the additive rule, and the watermarked image is encrypted by using the generated signature [13]. The specific algorithm is as follows.

(a) Performing first-order IWT decomposition on the carrier image P to obtain four sub-bands: LL, HL, LH, HH;

(b) Perform SVD conversion on the four sub-bands LL, HL, LH, and HH:

$P_i = U_iS_iV_i^T$,i represents the corresponding sub-band;

(c) Embedding the watermark information directly into the singular value of the corresponding subband of the carrier image P, applying the SVD transform to modify the odd of the corresponding subband.

(d) U, V matrix corresponding to LL, HL, LH, HH4 subbands (U_i^W and V_i^{TW}) after applying the signature generation program to generate four 8-bit digital signatures Sig_{LL}, Sig_{HL}, Sig_{LH}, Sig_{HH}, the XOR operation forms the final signature:

Watermark extraction process

Before extracting the watermark, the four subsets of U_i^W and V_i^{TW} after SVD decomposition of the received image are detected and authenticated. The process of authentication is to first generate a digital signature using the key and then match the digital signature extracted from the U_i^W of the received image and the four subsets of Vi^{WT}. If the digital signature matches, the watermark extraction process continues and the embedded watermark is extracted. Otherwise, it is considered a false alarm and the procedure is terminated. The specific steps of watermark extraction after digital signature matching are as follows.

(a) Performing a level 1 IWT decomposition on the received watermarked image P*W to generate four sub-bands LL, LH, HL, HH;

(b) Perform SVD operations on all subbands:

$P^{*W} =U^*_i S^*_iV^*_i$

(c) Calculate each subband as follows:

$B^*_i =U_i^WS^*_iV_iT^W$;

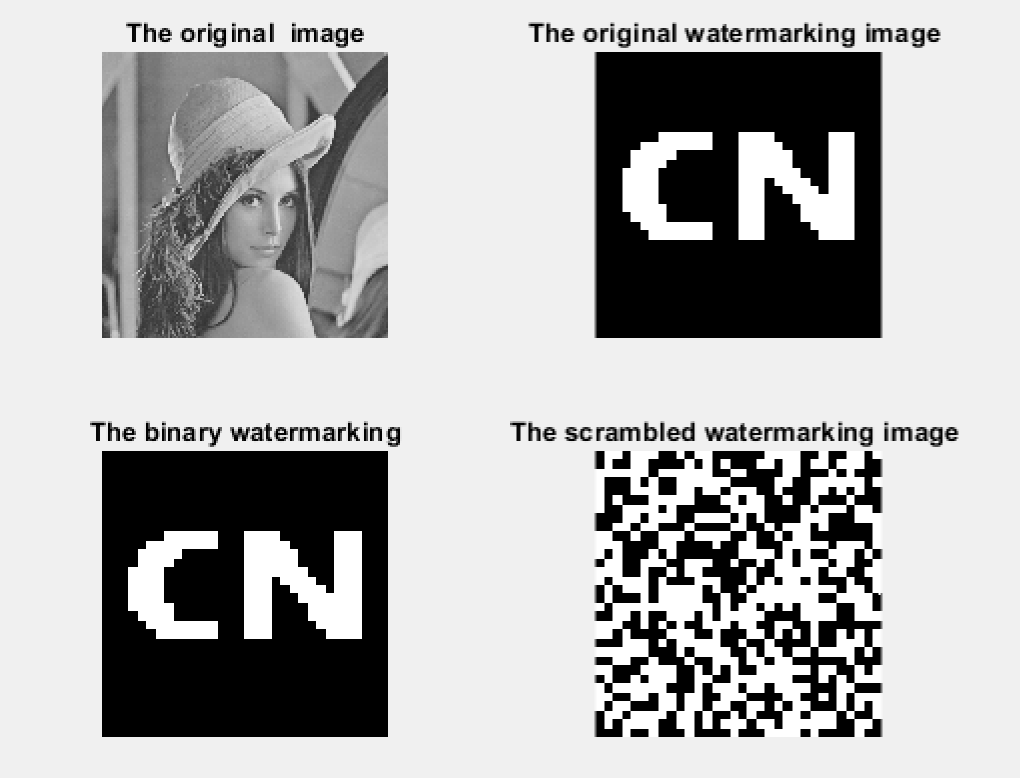
The original image
The original watermarking image
CN
The binary watermarking
CN
The scrambled watermarking image

Figure 1 Watermark image

3. EXPERIMENTAL RESULT

The algorithm in this paper was implemented using MATLAB 2018, and the image was tested in a 32-bit. The experiment uses a grayscale image of 512×512 Lena as the carrier image, and the watermark image is a 64×64 binary image, as shown in Fig.1. The visual and robustness of the algorithm are verified by different experiments.

Conventional Attacks

In order to further verify the robustness of the algorithm, adding Gaussian noise, JPEG compression to the image is performed on the algorithm (table 1).

Table 1 The NC under Conventional Attacks based on IWT-SVD.

Conventional attacks	Gaussian noise			JPEG Compression		
	2%	4`%	6%	5%	10%	15%
NC	0.86	0.92	0.85	0.90	0.88	0.95

Geometric Attacks

In order to further verify the robustness of the algorithm, adding Geometric Attacks to the image is performed on the algorithm (table 2).

Table 2 The NC under Geometric Attacks based on IWT-SVD.

Geometric Attacks	Attack strength	NC
Rotation (clockwise)	10^0 20^0 30^0	0.92 0.91 0.88
Rotation (Anticlockwise)	5^0 15^0 30^0	0.86 0.94 0.86
Scaling	× 0.6 × 0.8	0.82 0.88
Translation (Right)	5% 10% 20%	0.90 0.89 0.95
Translation (down)	8% 20% 25%	0.86 0.91 0.82
Clipping (Ydirection)	15% 20%	0.88 0.95
Clipping (X direction)	10% 20%	0.92 0.94

Compared to other algorithms Table 3 Show the robustness of the proposed algorithm to both technical and conventional attacks compared to IWT and SVD methods. The robustness of the watermarking algorithm improved by correcting rotation for rotation is superior to the watermarking algorithm.

Table 3 Comparison of the three algorithms

Attacks strength	NC		
	IWT	SVD	IWT-SVD
Rotation 10^0 (Clockwise)	0.65	0.32	0.92
Rotation 15^0 (Anticlockwise)	0.72	0.55	0.94
Scaling (×0.8)	0.42	0.72	0.88
Translation 20% (right)	0.76	0.40	0.95
Translation 20% (down)	0.55	0.68	0.91
Cropping 20% (Xaxis)	0.88	0.76	0.94
Cropping 20% (Y axis)	0.82	0.78	0.95
JPEG Compression (15%)	0.55	0.67	0.92
Gaussian noise (4%)	0.44	0.80	0.95

4. CONCLUSION

In practical applications, digital image watermarking technology requires both good transparency and robustness against various types of attacks. It also requires effective control of the false alarm probability during detection. In this paper, based on the advantages of fast decomposition and lossless reversibility of IWT, a digital signature mechanism is proposed for the traditional SVD method, and the image is encrypted while the watermark is embedded. The digital signature is verified before the watermark is extracted. If the signature is incorrect, the watermark cannot be correctly extracted, and the watermark cannot be extracted in the carrier image without the watermark embedded, thereby effectively. Overcome the problem of excessive false alarm rate in the traditional SVD method. Experiments show that the proposed algorithm has good visual and robustness.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCE

1. Joseph, Smitha. "Implementation of the Two Dimensional Integer Wavelet Transform for Transmission of Images." (2004).
2. Dai, Qianning, et al. "An Automatic Identification Algorithm for Encrypted Anti-counterfeiting Tag Based on DWT-DCT and Chen's Chaos." *International Conference on Artificial Intelligence and Security*. Springer, Cham, 2019.
3. Li, Xin-E., W. Ke, and Yan-qiu Cui. "A WPT and DCT Based Bi-watermarking Algorithm [J]." *Journal of Image and Graphics* 12.1 (2007): 61-67.
4. Ganic, Emir, and Ahmet M. Eskicioglu. "Robust DWT-SVD domain image watermarking: embedding data in all frequencies." *Proceedings of the 2004 Workshop on Multimedia and Security*. ACM, 2004.
5. Xiao, Tong, et al. "A Robust Algorithm of Encrypted Face Recognition Based on DWT-DCT and Tent Map." *International Conference on Cloud Computing and Security*. Springer, Cham, 2018.
6. Liu, Jun-jing, and Hua Jiang. "An improved watermarking algorithm for digital image based on DCT and SVD." *Comput Eng Sci* 31.1 (2009): 38-40.
7. Verma, Vibha, Vinay Kumar Srivastava, and Falgun Thakkar. "DWT-SVD based digital image watermarking using swarm intelligence." *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. IEEE, 2016.
8. Loukhaoukha, K., M. Nabti, and K. Zebbiche. "A robust SVD-based image watermarking using a multi-objective particle swarm optimization." *Opto-Electronics Review* 22.1 (2014): 45-54.
9. Zhu, Xinzhong, Jianmin Zhao, and Huiying Xu. "A digital watermarking algorithm and implementation based on

improved SVD." *18th International Conference on Pattern Recognition (ICPR'06)*. Vol. 3. IEEE, 2006.

10. Mishra, Anurag, et al. "Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm." *Expert Systems with Applications* 41.17 (2014): 7858-7867.
11. Ansari, Irshad Ahmad, Millie Pant, and Chang WookAhn. "Robust and false positive free watermarking in IWT domain using SVD and ABC." *Engineering Applications of Artificial Intelligence* 49 (2016): 114-125.
12. Ghazy, Rania A., et al. "An efficient block-by-block SVD-based image watermarking scheme." *2007 National Radio Science Conference*. IEEE, 2007.