Improvement of Imperceptibility Evaluation Method and Security of Non-Blind Digital Image Watermarking Technique

Jon Tae Bom, Kim Kyong Jin[1], Ri Hyo Il,HyonCholKim, Jang Un Ju
Faculty of Mathematics, **Kim Il Sung** University, Pyongyang, DPR Korea

ABSRACT

This paper presents the new digital image watermarking technique that has high imperceptibility and robustness against various geometric image attacks such as rotation attack and cropping attack using discrete wavelet transform (DWT) and singular value decomposition (SVD).In this paper, watermark logo is scrambled by 3D Arnold's cat mapping and Chebyshev mapping, then security of watermark logo is realized.And control parameters of chaos mapping are encrypted bythe proposed quantum resistant encryption technique.
Also in this paper, the suitable color image similarity evaluation method and the suitable embedding scaling factor using the relative vision characteristic of human are defined,computed and used in evaluation of imperceptibility.

Keywords:Image watermarking, Discrete wavelet transform(DWT), Cat mapping, Chebyshev mapping

1. Introduction

Robustness, imperceptibility, watermark capacity and efficiencyare used for evaluation of digital image watermarking algorithm[1].
In the past we used spatial domain watermarking algorithm such as bit plane decomposition method, but we are using and developing the frequency domain watermarking algorithm now.Images can be transformed from spatial domain to frequency domain by discrete wavelet transform (DWT) and singular value decomposition (SVD) etc[3].
Recently, the research of logo method using chaos mapping is intensifying in the aspect of image logo and the one of quantum resistant encryption against quantum computer's attacks is intensifying in the aspect of cryptography[2, 4].
This paper presents non-blind digital image watermarking technique using discrete wavelet transform and singular value decomposition, 3D Arnold's cat mapping and Chebyshev mapping, and new quantum resistant encryption.And we defined the color image similarity evaluation index for evaluation of imperceptibility.Also the suitable embedding scaling factor using the relative vision characteristic of human is computed.
The techniqueproposed in this paperhas very high robustness and imperceptibility against various geometric image attacks and random noises.And effective index for color image similarity evaluation is presented and the imperceptibility of algorithmproposed in this paper is evaluated.
DWT, singular value decomposition (SVD) and chaos encryption are used in this paper.
Discrete wavelet transform (DWT) is used a lot in image information processing because it is similar to the vision system of human. In watermarking technique, discrete wavelet transform (DWT) offers high robustness.Normally in watermarking algorithms using discrete wavelet transform (DWT), watermark is embedded on low frequency sub-band that has main information of cover image.Because low frequency sub-band of cover image is not changed by random noises.
Disadvantage of frequency domain watermarking algorithm is that embedding capacity is small and calculation time is very long[2].

[1]Corresponding Author Email Address: HC.Kim@star-co.net.kp

Watermark logo is scrambled by Arnold's cat mapping that is one of chaos encryption[2]. Watermark logo is scrambled by logistic mapping in watermarking scheme. Then control parameters are encrypted by RSA that is a traditional public key encryption[5].
Watermarking method by discrete cosine transform (DCT) and one by singular value decomposition (SVD) are presented[6]. Effective watermarking algorithms based on frequency domain of DWT-DCT, DCT-SVD are presented. Presented algorithm is tested by using various medical images for various random noises[6]. Signal watermarking method by SVD-DCT is presented and new evaluation indices are used[7]. Discrete cosine transform (DCT) is used for digital video watermarking. In digital video watermarking, each frame is watermarked and extracted[8].
In this paper, watermark logo areembedded on low frequency of cover image. So algorithm has high imperceptibility and high robustness against various image attacks and random noises.
Watermark logo is scrambled by 3D Arnold's cat mapping and Chebyshev mapping and control parameters of chaos mapping are encrypted by the proposed quantum resistant encryption.

2. New proposed contents

2.1 New setting of scaling factor

In the literature about the watermarking techniques,the embedding scaling factor is generally 0.05,sincewhen human distinguishes I from $I + dI$, $\frac{dI}{I} \geq 0.05$. But boundary of $\frac{dI}{I}$ in each channel is not same in color image. We can find it from the following expression changing color image into gray one.

$$I = 0.2989 * R + 0.5870 * G + 0.1140 * B$$

Where coefficients stand for the relative vision ratios for each channel in color image. So we will newly define the embedding scaling factor.
Let the scaling factors of R, G, B channels be α_r , α_g and α_b, respectively. In this paper, we set up the scaling factorsfor channels whose mean is 0.05.

$$\alpha_r : \alpha_g : \alpha_b = \frac{1}{0.2989} : \frac{1}{0.5870} : \frac{1}{0.1140} = 0.2421 : 0.1232 : 0.6347$$

$$\begin{cases} \alpha_r = 0.0363 \\ \alpha_g = 0.0185 \\ \alpha_b = 0.0952 \end{cases}$$

2.2Embedding process

STEP 1: Read the m × m cover image and the secret image whose shape is a square and whose size is high or less than the cover image.

STEP 2: Apply DWT to the cover image by HAAR basis to get four sub-bands *LLI, LHI, HLI*and*HHI*.

$$[LLI, LHI, HLI, HHI] = dwt2(I, 'haar')$$

STEP 3: Apply SVD to the *LLI* sub-band to get *UI, SI*and *VI*.

$$[UI, SI, VI] = svd(LLI, 'econ')$$

STEP 4:Add scrambled secret image *W* with scaling factorto the *LLI*.

$$LLI1 = LLI + \alpha \cdot W$$

STEP 5: Apply SVD to decompose *LLI1* sub-band to get *UI1* , *SI1* , *VI1*.

$$[UI1, SI1, VI1] = svd(LLI1, 'econ')$$

STEP 6: Reconstruct low frequency sub-band matrix that has watermark information *LLIw* by using *UI* , *SIw* and *VI*.

$$LLIw = UI \cdot SI1 \cdot VI^T$$

STEP 7: Construct watermarked image*Iw* by using *LLIw*.

$$Iw = idwt\,2(LLIw, LHI, HLI, Iw, 'haar')$$

Watermark logo is scrambled by 3D Arnold's cat mapping and Chebyshev mapping before it is embedded to the cover image for security.

2.3Extraction process

STEP 1: Read the m × m watermarked image *Iw*.

STEP 2: Apply DWT to the image *Iw*by HAAR basis to get four sub-bands *LLIwstar, LHI, HLI*and *HHI*.

$$[LLIwstar, LHIstar, HLIstar, HHIstar] = dwt2(Iwstar, 'haar')$$

STEP 3: Apply SVD to the *LLIwstar* to get three sub-bands *UI , SIw*and *VI*.

$$[UI, SIw, VI] = svd(LLIwstar, 'econ')$$

STEP 4: Construct LLIw by using *UI1 , SIw , VI1*

$$LLIw = UI1 \cdot SIw \cdot VI1^T$$

STEP 5: Construct scrambled secret image.

$$W = (LLw - LLI)/\alpha$$

Watermark logo is decrypted by inverse process of 3D Arnold's cat mapping and Chebyshev mapping after itis detected on cover image.Also, we encrypted the control parameters by using recently proposed quantum resistant encryption based on NTRU[9].

2.4 Improvement of evaluation index

Among three channels of color image, human vision about detailed changes of each channel is different. Concretely, human responds sensitively to thedetailed changes of G channel, but for R or B channel it does not. So when we assess the MSE of images, weight coefficient is notthe same.
The following graph(Fig.1) shows the comparative vision quantity of color with respect to wavelength.

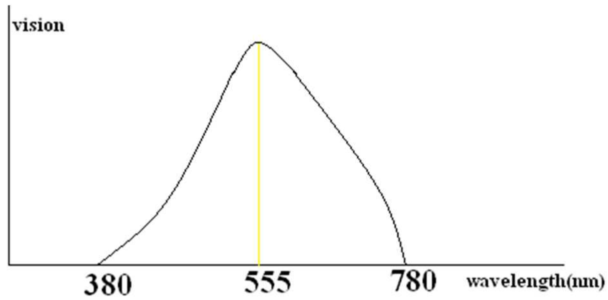


Fig.1

But it is very difficult to evaluate the weight coefficient in mathematical way.
So the mean square error (MSE) is defined by using the color distance of literature.The color distance in HSV color model is defined as follows.

$$cd(c_i, c_j) = |v_i - v_j| + \left| v_i s_i \cos\left(\frac{h_i}{3}\right) - v_j s_j \cos\left(\frac{h_i}{3}\right) \right| + \left| v_i s_i \sin\left(\frac{h_i}{3}\right) - v_j s_j \sin\left(\frac{h_i}{3}\right) \right|$$

In HSV color model,we defined CMSE and CPSNR based on the color distance as follows.

$$\mathrm{CM}SE = \frac{1}{n} \sum_{i=1}^{n} cd(P_i - Q_i)^2$$

$$CPSNR = 10\lg\left(\frac{peakval^2}{CMSE} \right)$$

In this paper, we propose the imperceptibility asa new evaluation index (CPSNR).

3. Experimental results

In this paper, we evaluate the algorithm in terms of imperceptibility, robustness, efficiency and watermark embedding capacity. CPSNR, SSIM and NC(Normalized correlation) are used in imperceptibility evaluation of the proposed algorithm. In this paper, weevaluatethe robustness against the geometric image attacks and the results of the cases ofvarious random noises and compression attacks are similar.

All of the experimentsaredone oncomputer which has an 12^{th} Gen Intel(R) Core i7-12700(20cpus) by means of MATLAB R2021acomparing withpreceding literature.

4.3.1 Imperceptibility Test

The imperceptibility is measured by calculating the CPSNR, SSIM and NC between the watermarked image and the original cover image. Table 1 shows the experimental results.As known in Table 1, when the watermark ofmaximum capacity isembedded in the original image, the imperceptibility is very high. Table2 shows comparative resultswithpreceding literature.

Table.1

	CPSNR	SSIM	NC
Value	104.1596	1.0000	1.0000

Table.2

	[2]	[11]	[12]	[13]	Proposed
SSIM	0.9991	0.9213	0.9952	0.9999	**1.0000**
NC	0.9999	-	-	-	**1.0000**

Next, the secret images of different sizes are tested on the proposed algorithm. Table 3 shows the results of square secret images of dimensions 32, 64 and 256. Table.3 shows the similarity between original cover image and watermarked image with respect to the length of watermark.

Table.3

	CPSNR	SSIM	NC
32×32	inf	1.0000	1.0000
64×64	inf	1.0000	1.0000
256×256	104.1596	1.0000	1.0000

Experimental results show that the algorithm proposedin this paper has high imperceptibility. The algorithm successfully embedded the smaller secret images in the cover image. Generally, the imperceptibility decreases as the secret image size increases. In practice, a higher scaling factor should be used in smaller secret images.

4.3.2 Robustness test

In this part,we show similarity value of watermark logoby various evaluation indiceswith respect to the rotation angle.

The robustness is measured by calculating the PSNR and NC between the extracted watermark image and the original watermark image, with or without attacks. The results of the robustness calculation are shown in Table 4 and Table 5.

Table. 4

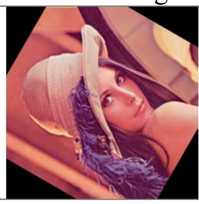
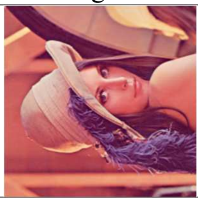
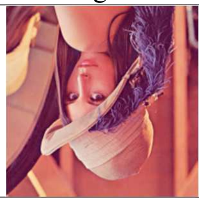
Theta	0	10	20	30	45	60
PSNR	46.2396	28.5384	28.2958	28.4790	28.1920	28.1367
NC	1.0000	0.9985	0.9983	0.9983	0.9984	0.9982

Table 5

angle	[2]	[14]	[10]	[12]	Proposed
10	0.9753	0.94	-	0.9873	**0.9885**

15	_	-	0.8419	-	**0.9784**
30	_	0.58	0.8256	-	**0.8983**
45	_	-	0.8304	-	**0.8574**
90	_	-	1.0000	-	**1.0000**
180	_	-	1.0000	-	**1.0000**

The below images(Fig.2-Fig.9) are the watermarked imageswhen being attacked with various rotation angle and theextracted watermark logos at that time.

	Rotated image	Extracted logo	Rotated image	Extracted logo
Image				
Image name	Fig.2	Fig.3	Fig.4	Fig.5
Image				
Image name	Fig.6	Fig.7	Fig.8	Fig.9

The above images show that proposed algorithm is very safe againstrotation attack.

4.3.3 Efficiency

In this part, we evaluate thetimeabout the embedding and extraction of watermark and Table.11 shows about them.. Result shows that the proposed algorithm is very fast. Table.12 shows about the detailed time in each step of proposed watermarking technique.

Table.6

	Embedding	Extraction
[2]	1.7970	2.2770
Proposed	**0.1437**	**0.0801**

Table.7

	scrambling	embedding	extraction	descrambling
Time	0.0654	0.0783	0.0562	0.0239

As shown in Table 7,we can know that it takes the shortest timein scrambling and descrambling of watermark logo.

4. Conclusion

The proposed digital image watermarking technique has been discussed in terms of imperceptibility, robustness against geometric attack, efficiency.

At present, communication technology is dramatically developing. So we mainly evaluated the robustness against various geometric image attacks.The results show that the algorithm is highly imperceptible and robust.

The proposed technique has high robustness and imperceptibility, high speed,because new scrambling method is used. Also, in this paper we use the quantum resistant encryption for security of control parameter. So encryption of watermark logo is very safe.Also, we newly defined the most suitable color image similarity evaluation index and evaluate the imperceptibility of algorithm.And the suitable embedding scaling factor was computed by using the relative vision characteristic of human.

The logo encoding method, color image similarity evaluation index and suitable embedding scaling factorwill be useful not only in watermarking but also in other image processing fields.

References

[1] Gaurav Kumar, Robust and Selective Watermarking using DWT, SVD and Image Depth Map, (IJCRT Volume 10, Issue 7 July 2022)832-844.

[2] Muhammad Khairi, A Razak, Kamilah Abdullah, Suhaila Abd Halim,Non-blind Image Watermarking Algorithm based on Non-Separable HaarWavelet Transform against Image Processing and Geometric Attacks, Journal of Advanced Research in Applied Sciences and Engineering Technology 29, Issue 2 (2022) 251 -267.

[3] Raviraj Singh Kurmi, Neha Khare, A Review. Digital Image Watermarking Techniques, International Journal of Recent Development in Engineering and Technology, (Volume 10, Issue 7, July 2021)16-20.

[4] Rameez Asif, Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms, IoT, 2021(2) 71-91.

[5] Yang Liu, Shanyu Tang, Ran Liu, Liping Zhang, Zhao Ma, Secure and robust digital image watermarking scheme using logistic and RSA encryption, Expert Systems With Applications, 97 (2018) 95–105.

[6] Jainul Aabdeed, DWT-DCT-SVD Based Biomedical Image Watermarking. Department of Electronics Engineering, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), Volume 17, Issue 1, Ser. I (Jan–Feb 2022)41-45.

[7] Bai Ying Lei, Ing Yann Soon, Zhen Li, Blind and robust audio watermarking scheme based on SVD–DCT, Signal Processing, 91 (2011)1973–1984.

[8] Ahmed Al-Gindy, A new watermarking scheme for digital videos using DCT, Open Computer Science, (2022; 12) 248 –259.

[9] C. Chen, O. Danba, J. Hoffstein, A. Hulsing, J. Rijneveld, J.M. Schanck, P. Schwabe, W. Whyte, Z. Zhang, NTRU: Algorithm Specifications and Supporting Documentation; Version September 2020, Available online: https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/submissions/NTRU-Round3.zip (accessed on 1 July 2022).

[10] Zunlin Fan, Low-level structure feature extraction for image processing via stacked sparse denoising autoencoder, Neurocomputing, 243 (2017) 12–20.

[11] Arjun Singh, A Hybrid Approach for Digital Watermarking Using DWT-SVD, International Journal of Innovative Research in Science Engineering and Technology (IJIRSET), (Volume 11, Issue 7, July 2022)10119-10132.

[12] Ahmadi, Sajjad Bagheri Baba, Gongxuan Zhang, Mahdi Rabbani, Lynda Boukela, Hamed Jelodar, An intelligentand blind dual color image watermarking for authentication and copyright protection, Applied Intelligence 51, No.3 (2021)1701-1732.

[13] Naffouti, Seif Eddine, Anis Kricha, and Anis Sakly, A sophisticated and provably grayscale image watermarkingsystem using DWT-SVD domain, The Visual Computer (2022)1-21.

[14] Yinghui Wang, A robust and blind 3D watermarking algorithm using multiresolution adaptive parameterization of surface,Neurocomputing, 237 (2017)304-315.