Color Image Watermarking in Encryption Domain

Rohit Thanki[1](✉) and Ashish Kothari[2]

[1] C. U. Shah University, Wadhwan City, Gujarat, India
rohitthanki9@gmail.com
[2] Atmiya University, Rajkot, Gujarat, India
amkothari@aits.edu.in

Abstract. Image watermarking is one of the techniques used for copyright protection of digital images. In this paper, copyright protection of color images using watermarking is presented with the help of data encryption. The main contribution in this algorithm is that the color image converts into an encrypted image using compressive sensing (CS) based encryption and then watermark logo is inserted into the encrypted image to get the watermarked encrypted image. After that, CS based decryption is applied to the watermarked version of an encrypted image to get a watermarked color image. Experimental results of this algorithm show that this technique effectively works for copyright protection of color images and provide better robustness compared to existing algorithms available in the literature.

Keywords: Compressive sensing · Color image · Encryption · Watermarking

1 Introduction

With the growth in social media in recent time, many images are transferred over social media is a very easy task. But sometimes images are transferred without any knowledge the actual creator or owner of it. This situation creates a problem regarding copyright protection of image and it is a very serious crime. The tackle with this crime, one of this technique is a digital watermarking [1]. In this technique, some secret information of creator hides into images or videos to prevent copyright protection of it [2]. Recently, many researchers are presented solution for copyright protection of images using different watermarking algorithms. The details of these algorithms are described as per below.

Savakar et al. [3] proposed hybrid watermarking algorithm based on DWT and SVD for color images. In this algorithm, U, V matrix values of wavelet coefficients of cover image are used for hides watermark into it with the help of PN sequences. This is blind extraction method. This algorithm provides robustness against all kind of attacks. Su et al. [4] proposed schur decomposition based watermarking algorithm for color images. Here, watermark hides into the approximate maximum value of schur coefficients of cover color image using weight factor to get the color watermarked image.

N. Chaubey et al. (Eds.): COMS2 2020, CCIS 1235, pp. 290–297, 2020.
https://doi.org/10.1007/978-981-15-6648-6_23

Bal et al. [5] proposed an image watermarking algorithm using cryptography where bit pair matching used for embedding and extraction of watermark image. This algorithm provides good invisibility with good payload capacity. Boris Escalated-Ramirez et al. [6] proposed Hermite transform (HT) based image watermarking algorithm. In this algorithm, the characteristics of HVS which is extracted using HT are used for generation of watermarked image while watermark mask is generated using brightness model. This algorithm provides robustness against all kinds of image watermarking attacks. Darwish et al. [7] proposed hybrid domain color image based intelligent watermarking algorithm using DWT + SVD and genetic algorithm (GA). Here, two watermarks are inserted into the singular values of Y channel and Cb channel of cover image with help of optimized scaling factor. The optimized scaling factor is generated with the help of a genetic algorithm.

Kazemivash et al. [8] proposed an image watermarking algorithm based on firefly optimization and lifting wavelet transform. In this algorithm, first, wavelet coefficients of the host image are selected using firefly optimization. Then, the encrypted watermark is inserted into this selected wavelet coefficients to get a watermarked image. For encryption of watermark, Arnold scrambling uses in this algorithm. Pan-pan et al. [9] proposed geometric feature extraction and LSB substitution based color image watermarking algorithm. In this algorithm, the color image feature is extracted using probability density gradient, Hessian matrix, and SURF feature extraction. After that, this feature divides into bit plane and the watermark is inserted into last bit plane with the help of LSB substitution to get the color watermarked image. Mehran Andalibi et al. [10] proposed an image watermarking algorithm based on wavelet transform and adaptive logo texturization. In this algorithm, first, texture feature of the host image is obtained with the help of HVS. Then adaptive iteration logo scrambling via Arnold transform is applied to the obtained similarity in texture feature. Finally, the watermark is inserted into these features with the help of wavelet based additive watermarking.

In this paper, compressive sensing (CS) based encryption is applied to the Y channel of host color image and converted into an encrypted for watermark content embedding. A logo watermark content along with PN sequence is embedded into the blocks of the encrypted image. In this proposed scheme of paper, logo watermark is inserted into an encrypted version of the color image indicates that this scheme is watermarking in the encryption domain. The paper is organized with Sect. 2 gives cs based encryption and decryption, Sect. 3 gives steps of the proposed scheme, Sect. 4 gives experimental results of the proposed scheme. Finally, Sect. 5 gives the conclusion of the obtained results of the scheme.

2 CS Based Encryption and Decryption

Compressive sensing is one kind of signal processing theory based on linear algebra and sparsity of data. This theory state that ‘signal or image can be recovered from its sparse few information’. This theory was introduced by D. Donoho and Candes around 2006 [11, 12]. Initially, this theory was proposed for the compression of data. After a few years of these, many researchers saw the use of this theory in the area of data encryption and decryption [13]. This theory provides simultaneously compression as well as encryption to data. The basic steps for encryption process and decryption process are described in the next subsection.

2.1 Encryption Process

The encrypted image is generated using sparse data of image and measurement matrix in this process. The basic steps of process are as follows:

Step 1: Sparse data (S) of image (I) is generated with help of transform basis function (Ψ).

$$S = \Psi \times I \times \Psi^{'} \tag{1}$$

Where S is sparse data of the image, Ψ is a transform basis function, and I is an original image.
Step 2: Measurement matrix (A) generates with the help of Gaussian normal distribution with mean value is zero and the variance value is one.
Step 3: Encrypted image generates by multiplication of sparse information and measurement matrix according to the below equation:

$$EI = A \times S \tag{2}$$

Where EI is an encrypted image.

2.2 Decryption Process

In this process, the encrypted image can be decrypted with the help of the measurement matrix and CS based recovery algorithms. These recovery algorithms are two types such as L norm based minimization and iterative based algorithm [14]. Here, the orthogonal matching pursuit algorithm [15] is used. The reason behind choosing this algorithm are that it is very simple and high simulation time compared to other recovery algorithms. The basic steps of process are as follows:

Step 1: The decrypted sparse data (x_R) of image from encrypted image (EI) can be get using orthogonal matching pursuit algorithm along with correct measurement matrix (A).

$$x_R = OMP(EI, A) \tag{3}$$

Step 2: After that, the decrypted image (DI) is generated with help of transform basis function (Ψ).

$$DI = \Psi^{'} \times x_R \times \Psi \tag{4}$$

3 Watermarking Algorithm

The watermark logo is inserted into encrypted color cover image to get color watermarked image while extraction of watermark from color watermarked image with the help of correlation properties of PN sequences. This algorithm has divided into processes such as embedding of watermark logo and extraction of watermark. The steps for these processes are described as per below:

3.1 Watermark Logo Embedding

The processing steps for embedding of watermark logo into the cover color image using below steps:

Step 1: The cover color image is taken, and the image converts into YCbCr colorspace using colorspace conversion of RGB to YCbCr.
Step 2: Y channel of the cover color image is chosen for the further process of watermark logo embedding.
Step 3: The encrypted Y channel of cover color image is generated using CS encryption process. Then, this encrypted channel of cover color image breaks into non-overlapping block with the size of 8 × 8.
Step 4: Two highly uncorrelated, random noise sequences are generated using PN sequence generator. The size of each sequence equals to block size.
Step 5: Then, the mask of watermark W is generated based on bits of watermark, size of encrypted channel of cover image and noise sequences using below steps:

- If watermark logo has a value of bit 1, then add noise sequence for one bit is added to that portion of mask.
- Otherwise, noise sequence for zero bit uses for generation of watermark mask.
- This process repeats for all blocks of encrypted channel of cover image.

Step 6: The watermark mask (W) is inserted into the encrypted Y channel of cover color image (EI) using weight factor (α) to get watermarked encrypted Y channel of the cover color image (WEI).

$$WEI = EI + \alpha \times W \tag{5}$$

Step 7: Apply CS based decryption watermarked encrypted Y channel to get watermarked Y channel of the cover color image.
Step 8: Finally, inverse colorspace conversion of YCbCr to RGB is performed to get a watermarked color image.

3.2 Watermark Logo Extraction

The steps for extraction of watermark logo from the watermarked color image are as per below:

Step 1: The watermarked color image is taken, and the image converts into YCbCr colorspace using colorspace conversion of RGB to YCbCr.
Step 2: Y channel of the watermarked color image is chosen for the further process of watermark logo extraction.
Step 3: The encrypted Y channel of watermarked color image is generated using CS encryption process. Then, this encrypted channel of watermarked color image breaks into non-overlapping block with the size of 8 × 8.
Step 4: Two highly uncorrelated, random noise sequences are taken which generates during watermark logo embedding process.

Step 5: The watermark bits' extract from watermarked encrypted Y channel of color image (*WEI*) using the following equations:

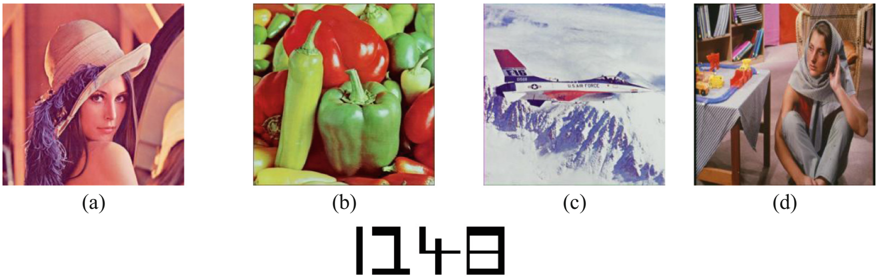
$$\begin{aligned} S_0 &= corr2(WEI,\ N_0) \\ S_1 &= corr2(WEI,\ N_1) \end{aligned} \tag{6}$$

Where *corr2* is a correlation, N_0 is a noise sequence for zero bit, and N_1 is a noise sequence for one bit.

Step 6: If $S_0 < S_1$, the set watermark bit as one bit. Otherwise, set watermark bit as zero bit. These extracted bits vector to obtain the extracted watermark logo.

4 Experimental Results

This watermarking algorithm is tested and analyzed using standard color image database which is taken from SIPI database [16]. The size of the color image is 256 × 256 pixels (shown in Fig. 1(a to d)). The binary watermark logo with a size of 50 × 20 pixels (shown in Fig. 1(e)). The quality of resultant image and performance of the proposed algorithm is measure using quality evaluation parameters [17] such as peak signal to noise ratio (PSNR), normalized correlation (NC), and structural similarity index measure (SSIM) [18]. The PSNR is used for impartibility of the algorithm while NC, SSIM are used for the robustness of the algorithm.

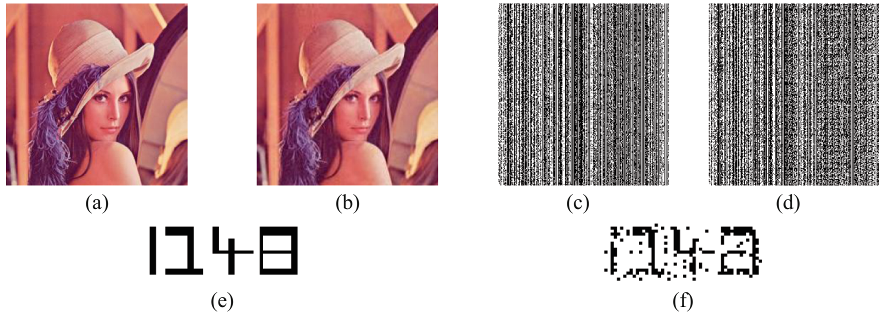


(a) (b) (c) (d)

(e)

Fig. 1. Test color image (a) lena (b) peppers (c) F16 airplane (d) barbara (e) watermark logo

Here, first, Y channel of the color image gets using RGB to YCbCr colorspace conversion. The CS based encryption is applied to the Y channel of a color image to get the encrypted Y channel of the color image. After that, the watermark mask is added to the encrypted Y channel of a color image with help of weight factor α. Then CS based decryption is applied on this resultant image to get watermarked encrypted Y channel of the color image. Finally, YCbCr to RGB color space conversion to get a watermarked color image. The resultant images using this proposed watermarking algorithm is shown in Fig. 2.


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

(e) (f)

Fig. 2. (a) Original lena image (b) watermarked lena image (c) encrypted Y channel of lena image (d) watermarked encrypted Y channel of lena image (e) original watermark logo (f) extracted watermark logo

Table 1 shows the quality parameters of the proposed watermarking algorithm for different weight factor values are summarized. The result in Table 1 shows that PSNR value is high for low weight factor while NC, SSIM value is high for high weight factor. The robustness of the proposed watermarking algorithm is tested and analyzed using various standard watermarking attacks such as JPEG compression, adding noise, filtering, geometric attacks such as rotation, cropping, blurring and histogram equalization. Table 2 summarized the NC and SSIM value of proposed watermarking algorithm against watermarking attacks. The results in Table 2 indicated that this algorithm provides robustness against watermarking attacks. The algorithm provides less robustness against filtering attacks and rotation attack.

Table 1. Quality parameters of proposed watermarking algorithm for different weight factors

Test images	K = 15			K = 30			K = 45		
	PSNR (dB)	NCC	SSIM	PSNR (dB)	NCC	SSIM	PSNR (dB)	NCC	SSIM
Lena	33.97	0.673	0.989	31.28	0.685	0.991	28.88	0.871	0.997
Pepper	33.78	0.759	0.992	31.26	0.764	0.993	29.14	0.829	0.996
F16 plane	32.33	0.660	0.989	30.40	0.740	0.991	28.62	0.757	0.992
Barbara	31.78	0.751	0.992	30.03	0.709	0.992	28.26	0.840	0.996

The robustness of the proposed watermarking algorithm is compared with the robustness of the recently published watermarking algorithm and summarized in Table 3. Here, the value of NCC is used for robustness performance of watermarking algorithms. The comparison result in Table 3 shows that this proposed algorithm provides better robustness compared to existing algorithms.

Table 2. NC and SSIM values of proposed watermarking algorithm against different watermarking attacks

Attacks	Lena		Peppers		F16 plane		Barbara	
	NCC	SSIM	NCC	SSIM	NCC	SSIM	NCC	SSIM
JPEG (Q = 90)	0.829	0.995	0.772	0.993	0.700	0.989	0.770	0.994
JPEG (Q = 80)	0.787	0.994	0.722	0.991	0.656	0.988	0.670	0.990
JPEG (Q = 60)	0.718	0.991	0.718	0.992	0.639	0.987	0.638	0.988
JPEG (Q = 50)	0.710	0.990	0.687	0.989	0.635	0.986	0.642	0.988
Gaussian noise (σ = 0.001)	0.849	0.996	0.813	0.995	0.741	0.992	0.833	0.995
Salt & pepper noise (σ = 0.005)	0.868	0.996	0.809	0.995	0.736	0.992	0.826	0.995
Speckle noise (σ = 0.005)	0.883	0.996	0.815	0.995	0.753	0.992	0.825	0.995
Median filter (3 × 3)	0.638	0.986	0.558	0.982	0.532	0.980	0.554	0.983
Mean filter (3 × 3)	0.452	0.975	0.410	0.972	0.410	0.972	0.526	0.981
Histogram equalization	0.887	0.997	0.849	0.996	0.817	0.995	0.829	0.995
Rotation (90°)	0.481	0.978	0.522	0.980	0.524	0.979	0.504	0.979
Cropping (20%)	0.872	0.997	0.829	0.996	0.756	0.992	0.841	0.996
Sharpening	0.912	0.998	0.845	0.996	0.797	0.994	0.854	0.996
Motion blurring	0.709	0.991	0.598	0.985	0.627	0.986	0.639	0.986

Table 3. Robustness compression of watermarking algorithms

Attacks	Pan-pan et al. [9]	Escalante-Ramirez et al. [6]	Bal et al. [5]	Proposed
JPEG	0.45	0.05	0.650	0.829
Gaussian	0.25	0.215	0.640	0.849
Speckle	Not reported	Not reported	0.840	0.868
Salt & peppers	Not reported	0.13	0.840	0.883

5 Conclusions

In this paper, the watermarking algorithm in the encryption domain has proposed, analyzed and simulated for a color image. Specifically, CS based encryption and decryption are used in this proposed algorithm for copyright protection of color images and results show that this algorithm can be used for this purpose. The comparison of algorithms is also indicated that the robustness of the proposed algorithm provides better than existing watermarking algorithms. This proposed algorithm is indicated that new way of watermark logo embedding.

References

1. Thanki, R.M., Kothari, A.M.: Digital watermarking: technical art of hiding a message. In: Intelligent Analysis of Multimedia Information, pp. 431–466. IGI Global (2017)
2. Borra, S., Thanki, R., Dey, N.: Digital Image Watermarking: Theoretical and Computational Advances. CRC Press, Boca Raton (2018)
3. Savakar, D.G., Ghuli, A.: Robust invisible digital image watermarking using hybrid scheme. Arab. J. Sci. Eng. **44**(4), 3995–4008 (2019)
4. Su, Q., Yuan, Z., Liu, D.: An approximate schur decomposition-based spatial domain color image watermarking method. IEEE Access **7**, 4358–4370 (2018)
5. Bal, S.N., Nayak, M.R., Sarkar, S.K.: On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching. J. King Saud Univ.-Comput. Inf. Sci. (2018)
6. Escalante-Ramírez, B., Gomez-Coronel, S.L.: A perceptive approach to digital image watermarking using a brightness model and the hermite transform. Math. Probl. Eng. **2018**, 19 (2018)
7. Darwish, S.M., Al-Khafaji, L.D.: An optimized dual watermarking scheme for color images. In: 2018 13th International Conference on Computer Engineering and Systems (ICCES), pp. 640–645. IEEE (2018)
8. Kazemivash, B., Moghaddam, M.E.: A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm. Multimed. Tools Appl. **76**(20), 20499–20524 (2016)
9. Pan-Pan, N., Xiang-Yang, W., Yu-Nan, L., Hong-Ying, Y.: A robust color image watermarking using local invariant significant bitplane histogram. Multimed. Tools Appl. **76**(3), 3403–3433 (2016)
10. Andalibi, M., Chandler, D.M.: Digital image watermarking via adaptive logo texturization. IEEE Trans. Image Process. **24**(12), 5060–5073 (2015)
11. Candès, E.J.: Compressive sampling. In: Proceedings of the International Congress of Mathematicians, vol. 3, pp. 1433–1452 (2006)
12. Donoho, D.L.: Compressed sensing. IEEE Trans. Inf. Theory **52**(4), 1289–1306 (2006)
13. Zhang, X., Ren, Y., Feng, G., Qian, Z.: Compressing encrypted image using compressive sensing. In: 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 222–225. IEEE (2011)
14. Thanki, R.M., Dwivedi, V.J., Borisagar, K.R.: Multibiometric Watermarking with Compressive Sensing Theory. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-73183-4
15. Tropp, J.A., Gilbert, A.C.: Signal recovery from random measurements via orthogonal matching pursuit. IEEE Trans. Inf. Theory **53**(12), 4655–4666 (2007)
16. The University of South Carolina SIPI Image Database. http://sipi.usc.edu/database/database.php. Accessed May 2019
17. Kutter, M., Petitcolas, F.A.: Fair benchmark for image watermarking systems. In: Security and Watermarking of Multimedia Contents, vol. 3657, pp. 226–240. International Society for Optics and Photonics (1999)
18. Malpica, W., Bovik, A.C.: SSIM based range image quality assessment. In: 4th International Workshop on Video Processing and Quality Metrics for Consumer Electronics (2009)