International Journal of Digital Crime and Forensics
Volume 13 • Issue 6

Reversible Data Hiding in a Chaotic Encryption Domain Based on Odevity Verification

Lianshan Liu, Shandong University of Science and Technology, Shandong, China
Xiaoli Wang, Shandong University of Science and Technology, Shandong, China
Lingzhuang Meng, Shandong University of Science and Technology, Shandong, China
Gang Tian, Shandong University of Science and Technology, Shandong, China
Ting Wang, Shandong University of Science and Technology, Shandong, China

ABSTRACT

On the premise of guaranteeing the visual effect, in order to improve the security of the image containing digital watermarking and restore the carrier image without distortion, reversible data hiding in chaotic encryption domain based on odevity verification was proposed. The original image was scrambled and encrypted by Henon mapping, and the redundancy between the pixels of the encrypted image was lost. Then, the embedding capacity of watermarking can be improved by using odevity verification, and the embedding location of watermarking can be randomly selected by using logistic mapping. When extracting the watermarking, the embedded data was judged according to the odevity of the pixel value of the embedding position of the watermarking, and the carrier image was restored nondestructively by odevity check image. The experimental results show that the peak signal-to-noise ratio (PSNR) of the original image is above 53 decibels after the image is decrypted and restored after embedding the watermarking in the encrypted domain, and the invisibility is good.

KEYWORDS

Chaotic Encryption System, Henon Mapping, Odevity Verification, Reversible Data Hiding

1 INTRODUCTION

More and more people were aware of the importance of protecting intellectual property rights. In order to protect their personal privacy and protect their legitimate rights and interests, they paid more and more attention to the protection of image property rights. Encryption technology and watermarking technology were two important means to protect multimedia digital information security and integrity. Reversible digital watermarking technology (Thodi & Rodriguez, 2007) was a new branch of digital watermarking technology. It could not only extract watermarking information correctly, but also restore the original carrier without distortion after extracting information. Therefore, it was widely used in sensitive areas such as medical images, military images and forensic images. Image encryption technology (Yun-peng et al., 2009) was to transform plaintext data into ciphertext data, which can reduce the risk of being stolen by others. How to combine encryption technology with

DOI: 10.4018/IJDCF.20211101.oa9

reversible watermarking technology to improve the reliability of embedding and extracting process was a subject worthy of study.

Reversible watermarking technology mainly included spatial domain algorithm (Xiao et al., 2019) (Ishtiaq et al., 2018) and transform domain algorithm. (Nguyen et al., 2016) Spatial domain algorithm mainly used redundancy between pixels to realize watermarking embedding, and transform domain algorithm used frequency of image to embedding watermarking. Reversible watermarking technology in encryption domain belonged to a special kind, it was encrypted in space domain and transform domain. Reversible data hiding of encrypted image was widely used in medical field(Kittawi & Al-Haj, 2017)(Parah & Ahad, 2018)(Abbasi & Memon, 2018). In the aspect of algorithm, for example, Zhang (2011) used the least significant bit method to embed the watermarking after excepting or encrypting the image in the spatial domain. Hong (2012) improved the above algorithm, making full use of the pixels calculated the smoothness of each block and the pixel correlation of adjacent block boundaries. Qian (2014) aimed to encrypt a JPEG bit stream into a properly organized structure, and embedded a secret message into the encrypted bit stream by slightly modifying the JPEG stream. Peng (2019) proposed an encryption domain RDH scheme for two-dimensional vector graphics based on real reversible mapping model (Bouridah et al., 2017)(Gao & Gao,). Encryption used chaotic mode to encrypt the image. After chaotic encryption, reversible data was hidden and extracted, which had higher security. But after encryption, the redundancy between the pixels of the image was lost, this situation resulted in the difficulty of watermarking embedding and the decreased of the embedding capacity of the watermarking. Zhang improved the watermarking embedding method of encrypted image and designed a special encryption scheme to encrypt the estimation error(Zhang et al., 2014). Later, a framework of RDH-EI based on Reversible Image Transform (RIT) was proposed to meet different image quality requirements and larger embedding capacity(Zhang et al., 2016). Aiming at the problem of low embedding capacity of encrypted image(Cao et al., 2016)(Choi & Pun, 2017), different high embedding capacity methods were adopted to improve the embedding capacity.

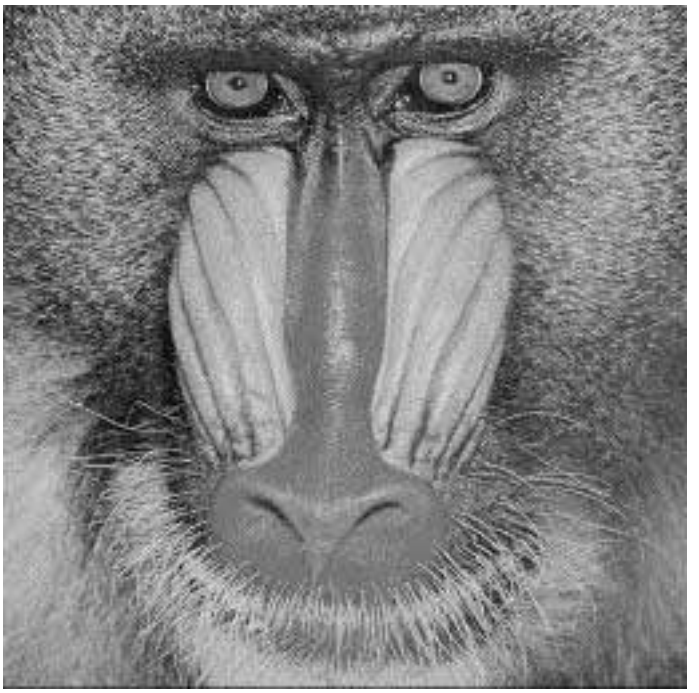
With the increase of image quality requirements, while extracting hidden data in encrypted domain, the quality of restored image should be guaranteed, and the reversible extraction of hidden data should be realized. Zhang (2012) proposed the reversible extraction of hidden data earlier. Ma (2013) used traditional RDH algorithm, a new method of reserving space before encryption was proposed, which maked it convenient for data hiding to embed data reversibly into encrypted images. Wu (2017) did not confine gray-scale images, but proposed a new RDH scheme for encrypted color images. In order to improve the security and quality of decrypted and restored images, a separable reversible data hiding method for encrypted images based on classified arrangement was proposed(Yin et al., 2017). The quality of decrypted and restored images could be significantly improved by utilizing spatial correlation. Vinoth Kumar (2019) proposed an effective method for recovering embedded data from tagged encrypted color images in the presence of attacks.

In order to solve the problem that image information was stolen by others and to protect its intellectual property rights, to better guarantee the undistorted restoration of original image and the security of encrypted image, and to improve the embedding capacity of watermarking, a chaotic encryption domain reversible watermarking algorithm based on odevity discrimination strategy was proposed in this paper. This algorithm could encrypt the digital image and used two mapping methods to mix encryption to improve the invisibility and security of the encrypted image. The adjacent pixels of the encrypted carrier image lose redundancy. Combining with odevity check strategy, the embedding capacity of the watermarking could be improved. Then the watermarking information could be embedded by reversible watermarking technology. The integrity of the watermarking could be used to judge whether the ciphertext was damaged or not, and finally the original image could be restored without distortion.

2 ENCRYPTION AND EMBEDDING OF WATERMARKS

Suppose the carrier image was an 8-level gray-scale image with the size of *M*N*, and the pixel value of each pixel was *I(i,j),1£ i£ M,1£ j£ N*. Let *W* be a binary image with the size of *P*Q*. The detailed process of encryption and embedding was shown in the following Fig. 1):

Figure 1. Flow chart of image encryption and watermarking embedding.



(1) The Henon map was used to generate X sequence and Y sequence. When $a\hat{I}$[1.07,1.4], b=0.3, the Henon map was in chaotic state. It could generate pseudo-random sequence, selected the value of *a*, and made the Henon map in chaotic state. Then it randomly selected *x1* and *y1* as (1) The Henon map was used to generate X sequence and Y sequence. When $a\hat{I}$[1.07,1.4], b=0.3, the Henon map was in chaotic state. It could generate pseudo-random sequence, selected the value of *a*, and made the Henon map in chaotic state. Then it randomly selected *x1* and *y1* as keys, and stores *a*, *x1* and *y1* in the key file.

$$\begin{cases} x_{n+1} = 1 + y_n - ax_n^2 \\ y_{n+1} = bx_n \end{cases} \tag{1}$$

(2)The original image I was scrambled by the X sequence generated by Henon mapping, and the scrambled image I^s was obtained.

Step 1: The *M*N* elements of the X sequence were intercepted and the sequence {*x1,x2... xM*N*} were obtained;

Step 2: The original image I was converted into a one-dimensional sequence *Ii* of *M*N*, and the data in the one-dimensional sequence *Ii* corresponded to the data in the sequence {*x1,x2...xM*N*}.

Step 3: Sequence {*x1,x2...xM*N*} was sorted in ascending order, and the corresponding element order of one-dimensional sequence was also changed.

Step 4: One-dimensional sequences were converted into two-dimensional *M*N* matrices, and scrambled images were obtained I^s.

The scrambled image I^s was encrypted by using Y sequence generated by Henon mapping, and a odevity check map PCM was generated according to the encrypted image.

Step 5: The *M*N* elements of Y sequence were intercept and the sequence {*y1,y2...yM*N*} were obtained;

{*y1,y2...yM*N*} was standardized in [0, 255] interval, and the *y'* was obtained.

$$k_1 = \frac{255}{y_{max} - y_{min}} \tag{2}$$

$$y_i^{'} = [k_1 * (y_i - y_{\min})], 1 \le i \le M * N \tag{3}$$

Each pixel value of scrambled image was converted to 8-bit binary number, which was expressed as;

$$b_{i,j}\left(k\right) = [\frac{I^s\left(i,j\right)}{2^{k-1}}] \bmod 2 \tag{4}$$

Step 8: The normalized sequence *yi* was converted into binary system, The $s_{i,j}(k)$ was obtained.

The image encryption was realized by excepting or encrypting $s_{i,j}(k)$ and $b_{i,j}\left(k\right)$, and the binary encrypted value $n_{i,j}(k)$ was obtained.

$$n_{i,j}(k) = b_{i,j}(k) \oplus s_{i,j}(k) \tag{5}$$

After converting the binary encryption value $n_{i,j}(k)$ into decimal, the decimal pixel value of the encrypted image I^e was obtained, and the size of the carrier image *M*N* was restored.

$$I^e(i,j) = \sum\nolimits_{k=1}^{8} n_{i,j}(k) * 2^{k-1} \tag{6}$$

The encrypted image I^e was even-digitalized, and the even-digitalized encrypted image I^{de} and odevity check graph PCM were generated, which were also stored in the key file.

$$I^{de}\left(i,j\right) = \left\lfloor \frac{I^e\left(i,j\right)}{2} \right\rfloor * 2 \tag{7}$$

$$PCM\left(i,j\right)=I^{e}\left(i,j\right)\bmod 2 \tag{8}$$

(3) The odevity check graph PCM was saved separately and stored in the key file.

The watermarking image W was embedded into the even-digitalized encrypted image, and the L sequence was generated by logistic mapping.

$$L_{k}+1=\mu L_{k}(1-L_{k}) \tag{9}$$

When 3.5699456...<μ<4, *L1*Î (0,1), the logistic map was chaotic, and the value of μ was selected to make the logistic map in chaotic state. Then, μ and *L1* were randomly selected as keys and stored in the key file. At this time, the key file contains *a, x1, y1, μ, L1* and odevity check PCM, which could be granted to different carrier images different keys;

(5) Logistic mapping was used to generate L sequence to select the embedding position, L sequence was standardized in [0, $M * N$] interval, and integrates L sequence. The first $P * Q$ values of L sequence were intercepted to embedd the watermarking, and the embedding position of the watermarking was obtained.

$$k_{2}=\frac{M*N}{L_{\max}-L_{\min}} \tag{10}$$

$$L_{i}^{'}=[k_{2}*(L_{i}-L_{\min})],1\le i\le P*Q \tag{11}$$

(6) The even-digitized encrypted image I^{de} and watermarking image W were transformed into one-dimensional sequence for data embedding.

$$I^{'}(L_{i}^{'})=I^{de}(L_{i}^{'})+W \tag{12}$$

If the embedding value was 1, the calculated value was odd, and if the embedding value was 0, the calculated value was even. When extracting data, the embedding value was 0 or 1 according to the odevity of the numerical value.

(7) One-dimensional sequences were transformed into two-dimensional matrices, the size of which was $M*N$, and the watermarked encrypted image I^{w} was obtained.

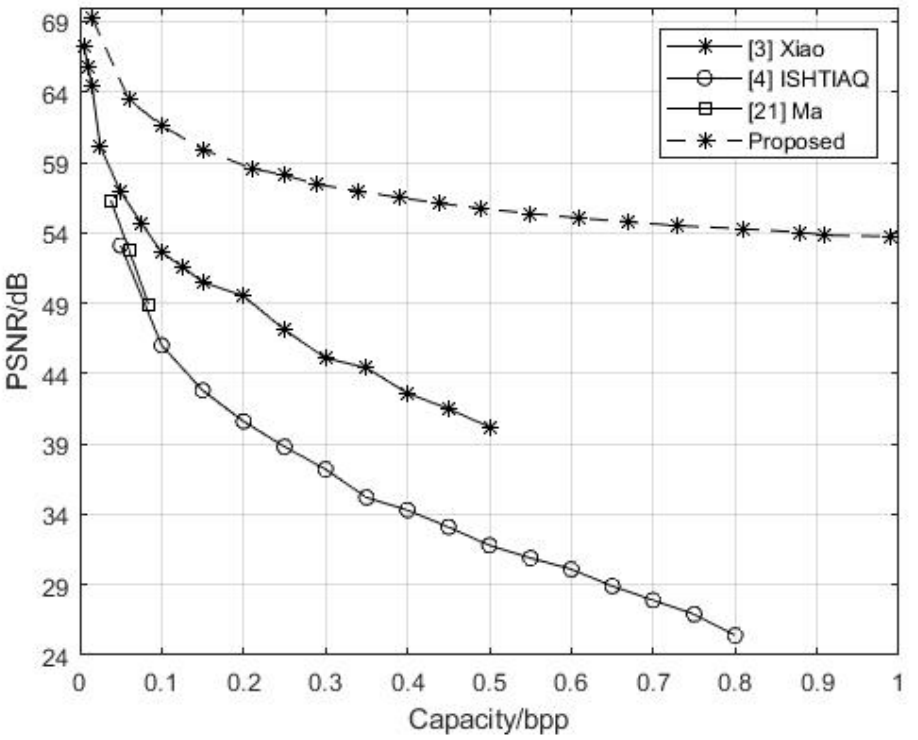
3 IMAGE DECRYPTION AND WATERMARKING EXTRACTION

According to the watermarked encrypted image, the size of the watermarked image $P*Q$ and the key file were decrypted. The process of decrypting and extracting watermarks was shown in the following Fig. 2):

(1) Logistic mapping was used to generate L sequence.

$$L_{k}+1=\mu L_{k}(1-L_{k}) \tag{13}$$

Figure 2. Flow chart of image decryption and watermarking extraction.



(2) The embedding position of the watermarking was copied by using L sequence. The sequence was normalized into [0, $M * N$] interval and the sequence was taken as L'. Firstly, the $P * Q$ value of the intercepted sequence was used to extract the watermarking, and the embedding position of the watermarking was obtained.

(3) The encrypted image of watermarking was converted into one-dimensional sequence. The watermarking data was extracted according to formula (14).

$$W = I'\left(L_i^{'}\right) \bmod 2, 1 \le i \le P * Q \tag{14}$$

After extracting the embedded data from one-dimensional digital sequence I', all that remains was the even-digitized encrypted image I^{de}.

(4) The watermarking image was restored, and the one-dimensional watermarking data W was transformed into two-dimensional matrix with the size of $P*Q$.

(5) Non-destructive restoration of even-digitized encrypted images I^{de} was performed, and undistorted encrypted images I^{e} were recovered by odevity-check PCM and I^{de}.

(6) The encrypted image I^{e} was decrypted, the X sequence and Y sequence are restored by Henon mapping and key *a, x1, y1, Y1* are substituted into Henon mapping formula (1), the X sequence and Y sequence are reproduced;

(7) The first decryption used Y sequence includes the following steps:

Step 1: The *M*N* elements of the Y sequence were intercepted and the sequence {*y1,y2... yM*N*} was obtained;
Step 2: {*y1,y2...yM*N*} was standardized in [0, 255] interval, and the *y*' was obtained.
Step 3: Each pixel value in the encrypted image I^e was converted, represented as $b'_{i,j}(k)$.

$$b'_{i,j}(k) = [\frac{I^e(i,j)}{2^{k-1}}] \bmod 2 \tag{15}$$

Step 4: y' was transformed to the $s_{i,j}(k)$.
Step 5: The image decryption was realized by using bit-by-bit XOR between $s_{i,j}(k)$ and $b'_{i,j}(k)$, and the image decryption was recorded as $n'_{i,j}(k)$

$$n'_{i,j}(k) = b'_{i,j}(k) \oplus s_{i,j}(k) \tag{16}$$

Step 6: For each deciphered pixel value $I^s(i,j)$, 1 < i < M, 1 < j < N was decimalized.

$$I^s(i,j) = \sum_{k=1}^{8} n'_{i,j}(k) * 2^{k-1} \tag{17}$$

(8) Secondary decryption of image used X sequence, included the following steps:
Step 7: The *M*N* elements of the X sequence were intercepted and the sequence {*x1,x2... xM*N*} were obtained;
Step 8: Scrambling images I^s were converted into one-dimensional sequences $I_1^s(i)$, 1 < i < *M*N*;
Step 9: A new sequence *Pos* was established to restore the scrambled image, and record the location of each *xi*, *Posi* = I.
Step 10: A new one-dimensional sequence H was established, which was used to carry the restored original image sequence.
Step 11: The intercepted sequence {*x1,x2...xM*N*} was sorted, according to the sequence value of *Posi* the scrambling image was restore;

$$H(Pos_i) = I_1^s(i) \tag{18}$$

Step 12: One-dimensional H sequence convert into a two-dimensional matrix of *M*N*, and the original image I was obtained.

4 EXPERIMENTAL RESULTS AND ANALYSIS

Four 512*512 gray images were selected: Lena, Baboon, Plane and Barbara. The watermark image was shown in the Fig. 3):

Firstly, they were scrambled, scrambling only changes the location of the pixels. Comparing the histogram of four original images and the histogram of scrambled images, we could see that the pixel value had not changed. Histogram comparison showed that this method was not safe. The original image and the scrambled image were the same. Some image features could be identified by statistical method. In order to increase the resistance of image recognition by statistical method, the image was encrypted in chaotic domain. By changing the pixel value of the image, the image could

Figure 3. Watermark image.

not be obtained through the statistical characteristics of the pixel value. Encrypted images could still remain invisible. The histogram value of the encrypted image changes and tended to be balanced, which reduced the risk of statistical recognition.

The scrambling operation of the original image made the image lose its visibility and guaranteed the security of the original image information. However, it also caused the redundancy between the pixels of the image to be lost. The general spatial algorithm could not be used, and the aberration expansion algorithm and histogram shifting algorithm were ineffective. However, scrambling was not safe enough. Statistical processing of the scrambled image histogram might still identify the image information resulted in tampering or loss of information. So it was necessary to encrypt the image information to make it more secure. Embedding personal information in the encrypted image guaranteed the intellectual property rights of one's own picture, which was used to guarantee one's legitimate rights and interests.

In order to expand the embedding capacity of the encrypted domain, the encrypted image could be odevity processed to make all the pixels into embeddable watermarking pixels and the increased embedding capacity of the watermarking. The generated odevity-check graph could be stored as a

Figure 4. a. Histogram of the original image, b. Histogram of scrambled Image, c. Histogram of encrypted Image.

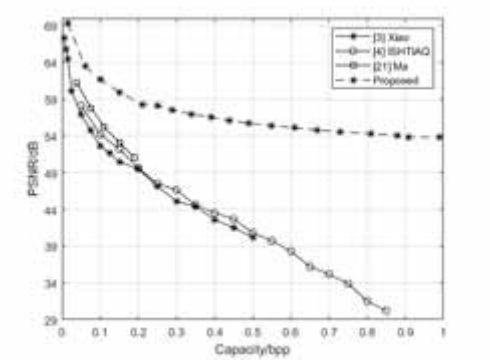


Figure 5. a. Original images b. Image scrambling using chaotic sequences, c. Encrypted images using chaotic sequences after scrambling, d. Embedded watermarked image after encryption, e. Extraction of watermark and restored Image after decryption.

key. After embedding the watermarking, the encrypted image embedded in the watermarking can be obtained. Then the watermarking of watermarked image can be extracted, decrypted and restored by key file, and the original image without distortion could be obtained, which could realize the reversible watermarking algorithm of the encrypted image well.

After the watermark extraction and image restoration of the image containing the watermark, the proposed watermark image was shown in the Fig. 6):

Because reversible watermark technology belongs to fragile watermark and has poor anti attack ability, the main performance test methods are peak signal-to-noise ratio and embedding capacity. PSNR was an objective criterion to measure image distortion or noise level. The bigger the PSNR value between the two images, the smaller the image distortion. The formula was as follows:

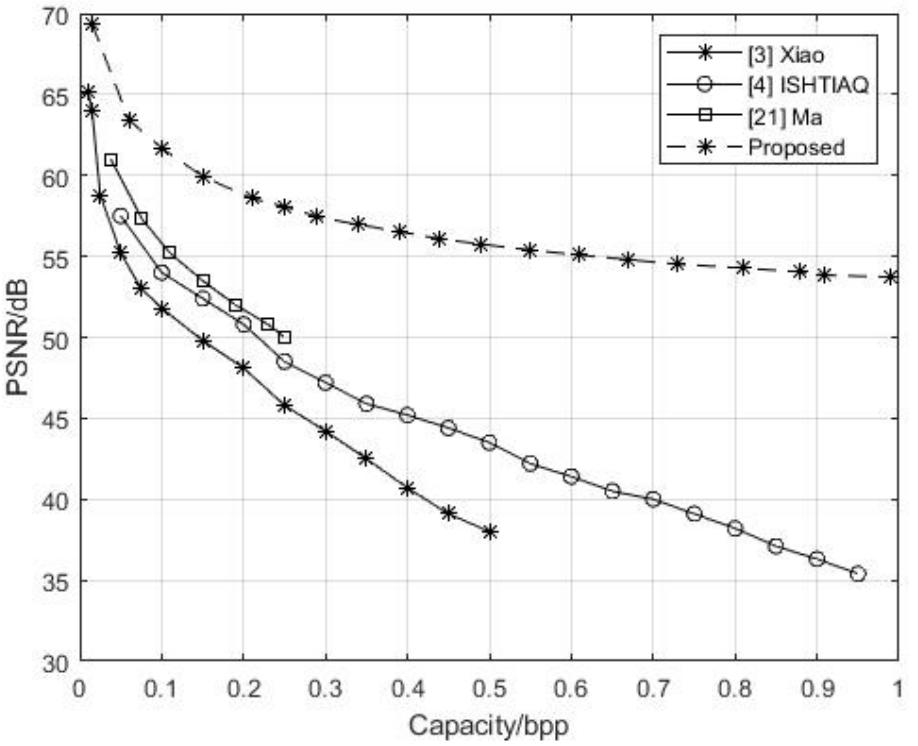
$$PSNR = 10 * \log_{10}(\frac{MAX^2}{MSE}) \tag{19}$$

MAX represents the maximum value of image color. MSE was the mean square error between I and K of m*n monochrome image. The definition formula was as follows:

$$MSE = \frac{1}{mn}\sum_{i=1}^{n}\sum_{j=1}^{m}\left\|K(i,j) - I(i,j)\right\|^2 \tag{20}$$

PSNR was used to evaluate the quality of the extracted watermarking and the recovered carrier image. The experimental results were as follows:

Figure 6. Proposed watermark image



From Table I and the experimental results, it could be seen that when the value of *L1* is fixed, the value of PSNR would decrease with the increase of embedding capacity, but it was higher than 53 dB as a whole, which shows that the image of embedded watermarking had good visibility and stable visual performance; when the embedding capacity was fixed, *L1* takes different values, and the peak signal-to-noise ratio was higher than 53. The ratio will fluctuate to a certain extent, but the overall fluctuation would not exceed 1. This showed that the embedding algorithm could guarantee the visibility of the image under different key conditions.

The experimental results in Fig.5 showed that the proposed algorithm could greatly increase the embedding capacity of the image. The maximum embedding capacity of each pixel bit was close to 1 bpp. The embedding capacity was higher than that of reference(Xiao et al., 2019)(Ishtiaq et al., 2018)(Ma et al., 2013). In different carrier images, the peak signal-to-noise ratio of reference (Xiao et al., 2019)(Ishtiaq et al., 2018)(Ma et al., 2013)decreased significantly with the embedding capacity. Although the peak signal-to-noise ratio (PSNR) of the proposed algorithm decreases with the increase of the embedding capacity, it decreased slightly and fluctuates slightly, and the overall PSNR was over 53. It showed that the proposed algorithm had good universality and good visual effect, and could be applied to a variety of images to ensure the quality of the restored image.

5 CONCLUSION

This algorithm belonged to the spatial domain watermarking algorithm, which had strong confidentiality and minimal modification of the image pixel value. First, original image used the

Table 1. Lena carrier image takes different l1 values (initial key value of logistic sequence) and peak signal-to-noise ratio (PSNR) under different embedding capacity

[REMOVED 610000491PUB-45EMBEDDED FIELD]Capacity /bpp	*L1*=0.01 PSNR/dB	*L1*=0.5 PSNR/dB	*L1*=0.8 PSNR/dB	*L1*=0.99 PSNR/dB
0.015	69.321	69.182	69.378	69.325
0.06	63.570	63.441	63.424	63.488
0.1	61.732	61.625	61.698	61.684
0.15	60.006	59.914	59.941	59.963
0.21	58.629	58.553	58.585	58.607
0.25	58.161	58.084	58.081	58.112
0.29	57.479	57.428	57.450	57.452
0.34	57.012	56.950	56.976	56.959
0.39	56.594	56.521	56.529	56.556
0.44	56.243	56.116	56.085	56.144
0.49	55.870	55.753	55.754	55.782
0.55	55.532	55.424	55.392	55.465
0.61	55.220	55.106	55.097	55.158
0.67	54.923	54.798	54.797	54.898
0.73	54.673	54.526	54.523	54.615
0.81	54.412	54.291	54.276	54.381
0.88	54.210	54.053	54.038	54.152
0.95	53.996	53.825	53.837	53.993
0.99	53.907	53.747	53.725	53.888

Figure 7. Performance comparison between our method and three methods of Xiao et al. (2019), Ishtiaq et al. (2019), Ma et al. (2013).

encrypted file to encrypt the image. Image encryption could not only ensure the privacy of the original image, reduce the possibility of the original image being attacked, but also did not depend on the redundancy between pixels. Combining odevity check graph could improve the embedding capacity of the watermarking, and then embedding the watermarking to ensured the property rights of the image. After extracting the watermarking, combined with the encrypted file, the image could be restored without distortion to achieve reversible watermarking. On the basis of high embedding

capacity, this method had high peak signal-to-noise ratio and tended to be stable, which guaranteed good visual effect and satisfies practical application.

ACKNOWLEDGMENT

This work was supported in part by National Natural Science Foundation of China (Grant No. 61702305); Project of Shandong Province Higher Educational Science and Technology Program (No. J17KA076).

REFERENCES

Abbasi & Memon. (2018). Reversible Watermarking for the Security of Medical Image Databases. *2018 21st Saudi Computer Society National Computer Conference (NCC),* 1-6.

Bouridah, Bouden, & Boulkroune. (2017). Image secure transmission using chaotic synchronization. *2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B),* 1-6.

Cao, X., Du, L., Wei, X., Meng, D., & Guo, X. (2016, May). High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation. *IEEE Transactions on Cybernetics*, *46*(5), 1132–1143. doi:10.1109/TCYB.2015.2423678 PMID:25955861

Choi, K., & Pun, C. (2017). Adaptive image encryption for high capacity reversible data hiding. *2017 IEEE Conference on Dependable and Secure Computing*, 429-432. doi:10.1109/DESEC.2017.8073862

Gao, , & Gao, . (n.d.). Double verifiable image encryption based on chaos and reversible watermarking algorithm. *Multimedia Tools and Applications*, *78*(6), 7267–7288.

Hong, , Chen, , & Wu, . (2012). An Improved Reversible Data Hiding in Encrypted Images Using Side Match. *IEEE Signal Processing Letters*, *19*(4), 199–202.

Ishtiaq, M., Ali, W., Shahzad, W., Jaffar, M. A., & Nam, Y. (2018). Hybrid Predictor Based Four-Phase Adaptive Reversible Watermarking. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 13213–13230. doi:10.1109/ACCESS.2018.2803301

Kittawi, N., & Al-Haj, A. (2017). Reversible Data Hiding in Encrypted Images. *2017 8th International Conference on Information Technology (ICIT)*. doi:10.1109/ICITECH.2017.8079951

Ma, K., Zhang, W., Zhao, X., Yu, N., & Li, F. (2013, March). Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption. *IEEE Transactions on Information Forensics and Security*, *8*(3), 553–562. doi:10.1109/TIFS.2013.2248725

Nguyen, T.-S., Chang, C.-C., & Yang, X.-Q. (2016). A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain. *AEÜ. International Journal of Electronics and Communications*, *70*(8), 1055–1061. doi:10.1016/j.aeue.2016.05.003

Parah, S. A., & Ahad, F. (2018). Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. *Journal of Biomedical Informatics*, *66*, 214–230.

Peng, , Lin, , Zhang, , & Long, . (2019). Reversible Data Hiding in Encrypted 2D Vector Graphics Based on Reversible Mapping Model for Real Numbers. *IEEE Transactions on Information Forensics and Security*, *14*(9), 2400–2411.

Qian, , Zhang, , & Wang, . (2014). Reversible Data Hiding in Encrypted JPEG Bitstream. *IEEE Transactions on Multimedia*, *16*(5), 1486–1491.

Thodi, D. M., & Rodriguez, J. J. (2007, March). Expansion Embedding Techniques for Reversible Watermarking. *IEEE Transactions on Image Processing*, *16*(3), 721–730. doi:10.1109/TIP.2006.891046 PMID:17357732

Vinoth Kumar, C., Natarajan, V., Nirmala, K., Balasubramanian, T., Ramnarayan Rao, K., & Krishnan, S. (2019). Encrypted separable reversible watermarking with authentication and error correction. *Multimedia Tools and Applications*, *78*(6), 7005–7027. doi:10.1007/s11042-018-6450-2

Wu, H., Shi, Y., Wang, H., & Zhou, L. (2017, August). Separable Reversible Data Hiding for Encrypted Palette Images With Color Partitioning and Flipping Verification. *IEEE Transactions on Circuits and Systems for Video Technology*, *27*(8), 1620–1631. doi:10.1109/TCSVT.2016.2556585

Xiao, Li, & Wang. (2019). Reversible data hiding based on pairwise embedding and optimal expansion path. Signal Processing, 158, 210-218.

Yin, B., Chen, F., He, H., & Yan, S. (2017). Separable Reversible Data Hiding in Encrypted Image with Classification Permutation. *2017 IEEE Third International Conference on Multimedia Big Data (BigMM)*, 201-204. doi:10.1109/BigMM.2017.48

Yun-peng, Z., Wei, L., Shui-ping, C., Zheng-jun, Z., Xuan, N., & Wei-di, D. (2009). Digital image encryption algorithm based on chaos and improved DES. *2009 IEEE International Conference on Systems, Man and Cybernetics*, 474-479. doi:10.1109/ICSMC.2009.5346839

Zhang. (2011). Reversible Data Hiding in Encrypted Image. *IEEE Signal Processing Letters, 18*(4), 255-258.

Zhang, W., Ma, K., & Yu, N. (2014). Reversibility improved data hiding in encrypted images. *Signal Processing*, *94*, 118–127. doi:10.1016/j.sigpro.2013.06.023

Zhang, W., Wang, H., Hou, D., & Yu, N. (2016, August). Reversible Data Hiding in Encrypted Images by Reversible Image Transformation. *IEEE Transactions on Multimedia*, *18*(8), 1469–1479. doi:10.1109/TMM.2016.2569497

Zhang, X. (2012, April). Separable Reversible Data Hiding in Encrypted Image. *IEEE Transactions on Information Forensics and Security*, *7*(2), 826–832. doi:10.1109/TIFS.2011.2176120

Liu Lianshan received a master's degree in control theory and control engineering from Shandong University of Technology in 1999 and a doctorate in control science and engineering from Xi'an Jiaotong University in 2006, China. From 2005 to 2019, he was an associate professor at the College of Computer Science and Engineering, Shandong University of Science and Technology. His research interests include digital image processing, information hiding, image authentication and pattern recognition. He is the member of China Computer Federation(CCF).

Wang Xiaoli is a graduate student at College of Computer Science and Engineering, Shandong University of Science and Technology. He works in the Digital Image Processing Laboratory. He is mainly engaged in image processing and digital watermarking technology.

Meng Lingzhuang was born in 1997. He is a graduate student at College of Computer Science and Engineering, Shandong University of Science and Technology. He works in the Digital Image Processing Laboratory, and mainly engaged in image processing and digital watermarking technology.

Tian Gang was born in 1982. He is a lecturer at College of Computer Science and Engineering, Shandong University of Science and Technology, and the member of China Computer Federation(CCF) . His research interests include Web service discovery, transfer learning, feature engineering, and knowledge extraction.

Wang Ting received her PhD degree and Master Degree in Computer Application Technologies from Ocean Universiy of China, Qingdao, China. She is currently a Lecturer at College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, China. Her main research interests include image processing, facial recognition, machine learning. She is a member of China Computer Federation.