Cryptanalysis of a Hamming Code and Logistic-Map based Pixel-Level Active Forgery Detection Scheme

Oussama Benrhouma
Faculty of Computer and Information Systems
Islamic University of Medinah, Medinah, KSA

***Abstract*—In this paper, we analyze the security of a fragile watermarking scheme for tamper detection in images recently proposed by S. Prasad et al. The chaotic functions are used in the scheme to exploit its pseudo-random behavior and its sensibility to initial condition and control parameter, but despite that, security flaws have been spotted and cryptanalysis of the scheme is conducted. Experimental results shows that the scheme could not withstand the attack and watermarked images were manipulated without triggering any alarm in the extraction scheme. In this paper, two different approaches of attacks are demonstrated and conducted to break the scheme. This work falls into the context of improving the quality of the designed cryptographic schemes taking into account several cryptanalysis techniques.**

***Keywords*—Cryptanalysis; watermarking; tamper detection; attack; chaotic functions; forgery localization**

I. Introduction

Nowadays we are living in the era of technology, and with a huge leap of internet technology the advancement is going faster and faster thanks to the easy and fast exchange of information, this makes led to the emergence of powerful software and hardware. Powerful devices with huge computational capacity became available at reasonable prices.

The amount of data exchanged via the internet is huge, multimedia contents represent a big percentage of these files, and with the presence of powerful and easy to use software the manipulation of these files became easier. With more than 300 million images uploaded every single day, the protection of these images became a necessity since it can be used to spread fake news, create problems between individuals or even nations, and now digital images could be presented as evidence in courtrooms. for these reasons, the scientific community is facing the challenge to present efficient solutions to control the integrity of these images.

Digital watermarking present a solution for these problems [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19]. Digital watermarking could be classified into three categories: robust, fragile, and semi-fragile watermarking schemes.

Robust watermarking schemes are typically designed for copyright protection [20], [21], [22]. The owner should be able to extract and verify an embedded watermark even from a falsified image, on the other hand, Fragile and semi-fragile watermarking schemes are designed to control the integrity of the cover image [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [18], [19], any unauthorized modification on the watermarked image should affect the embedded watermark and therefore detected by the legitimate receiver. The legitimate receiver is typically whoever possesses the secret key(s) to extract the watermark, and despite that the schemes are protected by secret key(s), successful attacks on these schemes has been conducted and the watermarks has been removed without possession of the key(s) [33], [34], [35], [36], [37]. The work presented by the cryptanalysts helped improving the quality of the future proposed security schemes. In this context w analyze the security of a recently proposed fragile watermarking scheme by S. Prasad et al [1], security flaws have been spotted in the scheme and two different types of attacks are performed and we were able to modify the image without being detected by the detection scheme, finally, an improvement of the scheme is proposed to cover the security problems.

The rest of the paper is organized as follows: In Section 2 we present a description of the scheme under study, Section 3 two types of attack are demonstrated and results are presented, finally, the paper is concluded in Section 4.

II. The Scheme under Study

The scheme in [1] proposes a fragile watermarking scheme for tamper detection in digital images. The scheme is based on (7,4) hamming code and logistic map: for each pixel the 4 most significant bits (MSBs) are selected and (7,4) hamming code is used to generate 3-bits authentication code that is then further processed using the logistic map and embedded into the LSBs of the pixel in question. In this section we present a brief description of the scheme under study.

A. Authentication Watermark Generation and Embedding

Given a cover image I with size $(M \times N)$ the steps leading to the generation and the embedding of the watermark are as follows:

Step 1: The logistic map is used to generate a pseudo-random sequence α where $\alpha = \{\alpha_i; i = 1 : (M \times N)\}$.
The Logistic map is defined by equation 1.The values generated by the equations are in [0,1], α_0 represents the initial condition provided by the user, and β is the control parameter of the function, where $\beta \in [0, 4]$.

$$\alpha_{i+1} = \beta\alpha_i(1 - \alpha_i) \quad (1)$$

The initial condition α_0 and the control parameter β are considered as secret keys of scheme.

Step 2: At this point we have a pseudo-random sequence $\alpha = \alpha_i \quad (i = 1 : MN)$, with the same size of

the image, each value from the sequence α will be associated to a pixel, where i represent the index of the pixel in processing.
The pseudo-random sequence is then converted to be in the range from 0 to 7 using the equations 2, 3 and 4.

$$A_i = \alpha_i \times 255 \tag{2}$$

$$B_i = round(A_i) \tag{3}$$

$$K_i = mod(B_i, 8) \tag{4}$$

Step 3: The i^{th} pixel in the cover image I is selected, converted to binary then its 4 MSBs are selected to compute its hamming code $c = (c_7, c_6, c_5, c_4, c_3, c_2, c_1)$.
The watermark is considered the 3 LSBs of the calculated hamming code: $W = (c_3, c_2, c_1)$

Step 4: The computed watermark is converted into an integer to obtain T.

Step 5: Starting from the secret value K_i a list R is created:

$$R = \{K_i, (K_i + 1)\ mod\ 8, (K_i + 2)\ mod\ 8, ..., (K_i + 7)\ mod\ 8, \} \tag{5}$$

Step 6: The value of the watermark T is Searched within the list R and its position in R is saved as "j".

Step 7: Calculate $z = mod\,(P_i, 8)$. Where P_i is the pixel in processing.

Step 8: Calculate list PR, where $PR = \{P_i - z + t\,;\, t = 0, 1, 2..., 7\}$.

Step 9: The watermarked pixel is represented by the j^{th} element in the list PR.

Step 10: The rest of the cover image is processed by applying the steps 3 to 9 to obtain the watermarked image WI.

A flowchart of the embedding schemes is shown in Fig. 1.

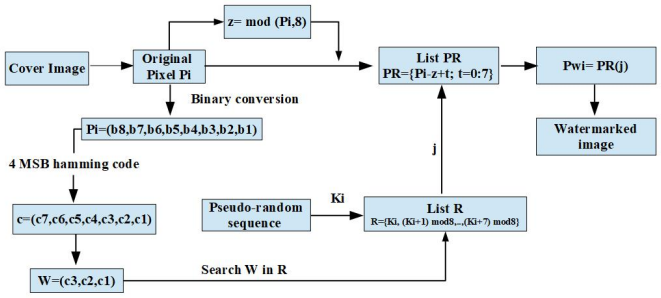


Fig. 1. Flowchart of the Embedding Phase [1]

B. Extraction and Tamper Detection

Given a received watermarked image WI. The steps leading to the extraction of the watermark in order to locate any possible tampering in the image are described as follows:

Step 1: Generate the same pseudo-random sequence α using the logistic map defined in equation 1 with the parameters α_0 and β as secret keys keys.
$\alpha = \{\alpha_i\ ;\ i = 1 : (M \times N)\}$. where $(M \times N)$ is the size of the image WI.

Step 2: The pseudo-random sequence α is then converted to be in the range from 0 to 7 using the equations 2, 3 and 4.
The list K with the same size as the image and each element represents the secret value that will be used to generate the list R for each pixel.

Step 3: The i^{th} pixel P_{Wi} in the received image WI is selected, then converted to binary then its 4 MSBs are selected to compute its hamming code $c = (c_7, c_6, c_5, c_4, c_3, c_2, c_1)$.
The 3-bits authentication code watermark is the 3 LSBs of the calculated hamming code c: $W = (c_3, c_2, c_1)$

Step 4: The list R is generated starting from the elements of the list K: for the i^{th} pixel the element K_i is used to calculate the list R:

$$R = \{K_i, (K_i + 1)\ mod\ 8, (K_i + 2)\ mod\ 8, ..., (K_i + 7)\ mod\ 8, \} \tag{6}$$

Step 5: Compute $z = mod\,(P_{Wi}, 8) + 1$ which represents the index of the extracted watermark E_{AC} in the list R.

Step 6: The comparison between the extracted watermark E_{AC} and the calculated one W will reveal if the pixel in question has been tampered with: each pixel where $E_{AC} \neq W$ is considered falsified, therefore its position in the received image is set to zero which represent the black color.

A flowchart of the extraction and tamper detection schemes is shown in Fig. 2.

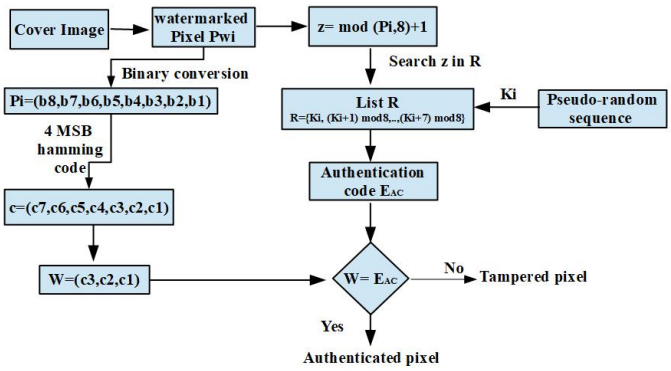


Fig. 2. Flowchart of the Extraction Phase [1]

III. Cryptanalysis of the Scheme

A. Offline Attack

In general, an attacker's goal is is either to guess or recover the value of the secret key(s) or something equivalent to the key(s) in order to recover the plaintext without knowledge of the secret key and that is due to kerckhoff's principle that states

that everything about the cryptosystem is public knowledge except for the keys.

In other words, the only thing secret about a cryptosystem is the secret key(s), everything else should be known and the job of a cryptographer is to design a cryptosystem that stands against any type of attack taking into consideration Kerckhoff's law [38].

The scheme under study [1] is a fragile watermarking system for tamper detection in digital images, after a successful cryptanalysis we should be able to manipulate the watermarked images without being detected by the extraction scheme. To achieve that goal, the keys or the equivalent of the keys are needed.

In the scheme in [1] the keys are the initial condition α_0 and the control parameter β of the logistic map.

The keys $(\alpha_0, beta)$ are used to generate a pseudo-random sequence α with the same size of the image then the sequence is quantified to be in the range of [0,7] to obtain the sequence K ad each element K_i in K is assigned to the pixel i in the image and the sequence R is constructed : $R = \{K_i, (K_i + 1)mod\,8, (K_i + 2)mod\,8, ..., (K_i + 7)mod\,8\}$

One of the main features of the chaotic maps is the high sensibility to initial conditions and control parameter, which make the attempt of any prediction or guess to their values starting from the pattern of the function nearly impossible, beside the pattern of the function is not available, but we know that it has been used to construct the lists K and R.

Since that the main keys are very hard to find our goal is to reveal alternative keys which are the lists R for each pixel we attempt to modify, and the list K if needed in any other attack intercepted from the same source.

In this section we will demonstrate how to reveal the list R for each pixel and as a result we will be able to construct the list K for the image:

Given an intercepted watermarked image "WI" with size $M \times N$, the steps leading to the revelation of the lists R and K are as follows:

Step 1: The i^{th} pixel P_{Wi} in the intercepted watermarked image WI is selected, then converted to binary then its 4 MSBs are selected to compute its hamming code $c = (c_7, c_6, c_5, c_4, c_3, c_2, c_1)$.
The 3-bits authentication code watermark is the 3 LSBs of the calculated hamming code c: $W = (c_3, c_2, c_1)$
It should be noted that i represents the index of the pixel in the image : $i = 1 : M * N$.

Step 2: Compute $z = mod\,(P_{Wi}, 8)$ which represents the index of the watermark W in the list R.

Step 3: Starting from the z^{th} position, the list R could be reconstructed using equation 7.

$$R((z+j)mod8) = (W+j)mod8 \quad where j = 0 : 7. \tag{7}$$

It should be noted that the authors in [1] used $z = mod\,(P_{Wi}, 8) + 1$ based on the indexation starts from 1 not 0, in our attack we dealt with the lists from 0 to 7 indexation.

Step 4: The first element in the list R represents the value K_i in the pseudo random-sequence K.
Once all pixels of the intercepted image are processed the pseudo-random sequence K is revealed.

Step 5: The i^{th} pixel could now be modified and the watermark is substituted with the new one with the possession of the list R.

With the possession of the equivalent keys (The lists R and K), the watermarked image could now be manipulated and the watermark is replaced without being detected by the extraction scheme. Next we present two examples how to calculate the list R for a given pixel and find the corresponding value K_i.

a) Example 1:: In the first example the value of the pixel $P_i = 165$ and $K_i = 3$.

First the watermark embedding process:

1) The list R is constructed using equation 5

$$R = \{K_i, (K_i+1)mod8, (K_i+2)mod8, ..., (K_i+7)mod8, \}$$

$$\Rightarrow R = \{3, 4, 5, 6, 7, 0, 1, 2\}$$

2) Calculate $z = mod\,(P_i, 8) \quad \Rightarrow z = mod(165, 8) = 5$.

3) Calculate list PR, where $PR = \{P_i - z + t\,;\, t = 0, 1, 2..., 7\}$.
$\Rightarrow PR = \{160, 161, 162, 163, 164, 165, 166, 167\}$.

4) P_i is converted to binary and the hamming code c for its 4 MSBs is calculated:
$\Rightarrow (165)_{10} = (10100101)_2$
$\Rightarrow c = H_{(4,7)}(1010) = 1010010 \Rightarrow T = (c_3, c_2, c_1) = (010)_2 = 2_{10}$.

5) Search for T_{10} in R and and its position in PR is considered as watermarked pixel: $R = \{3, 4, 5, 6, 7, 0, 1, 2\}; \quad T = 2_{10} \Rightarrow 7^{th} position$
$PR = \{160, 161, 162, 163, 164, 165, 166, 167\} \Rightarrow P_{Wi} = PR(7) = 167$

The image is then intercepted during transmission, next we demonstrate how the list R is calculated along with the value K_i.

1) $P_{Wi} = 167$ is the value of the ith pixel in the intercepted watermarked image "WI"
P_{Wi} is then converted to binary and the hamming code is calculated for its 4 MSBs to obtain T.
$\Rightarrow (167)_{10} = (10100111)_2$
$\Rightarrow c = H_{(4,7)}(1010) = 1010010 \Rightarrow T = (c_3, c_2, c_1) = (010)_2 = 2_{10}$.

2) Calculate $z = mod\,(P_{Wi}, 8) \Rightarrow z = mod(167, 8) = 7$.
This means that the z^{th} position in R contain the value of T.
$\Rightarrow R(7) = 2; \Rightarrow R = \{?, ?, ?, ?, ?, ?, ?, 2\}$

3) The list R is now constructed using equation 7.
$R((z+j)\,mod8) = (W+j)\,mod8 \quad where j = 0 : 7$
$\Rightarrow R(7) = 2; R(0) = 3; R(1) = 4; R(2) = 5; R(3) = 6; R(4) = 7; R(5) = 0; R(6) = 1$
$\Rightarrow R = \{3, 4, 5, 6, 7, 0, 1, 2\}$

4) The first element in the list R represents the value K_i where i is the index of the pixel in question : $K_i = 3$.
5) The i^{th} pixel could now be modified and the watermark substituted with the possession of the list R.

b) Example 2:: In the second example the value of the pixel $P_i = 99$ and $K_i = 5$.

First the watermark embedding process:

1) The list R is constructed using equation 5

$$R = \{K_i, (K_i+1)mod8, (K_i+2)mod8, ..., (K_i+7)mod8, \}$$

$\Rightarrow R = \{5, 6, 7, 0, 1, 2, 3, 4\}$
2) Calculate $z = mod(P_i, 8) \quad \Rightarrow z = mod(99, 8) = 3$.
3) Calculate list PR, where $PR = \{P_i - z + t\ ;\ t = 0, 1, 2..., 7\}$.
$\Rightarrow PR = \{96, 97, 98, 99, 100, 101, 102, 103\}$.
4) P_i is converted to binary and the hamming code c for its 4 MSBs is calculated:
$\Rightarrow (99)_{10} = (01100011)_2$
$\Rightarrow c = H_{(4,7)}(0110) = 0110011 \Rightarrow T = (c_3, c_2, c_1) = (011)_2 = 3_{10}$.
5) Search for T_{10} in R and and its position in PR is considered as watermarked pixel:
$R = \{5, 6, 7, 0, 1, 2, 3, 4\}; \quad T = 2_{10} \Rightarrow 6^{th} position$
$PR = \{96, 97, 98, 99, 100, 101, 102, 103\} \Rightarrow P_{Wi} = PR(6) = 102$

The image is then intercepted during transmission, next we demonstrate how the list R is calculated along with the value K_i.

1) $P_{Wi} = 102$ is the value of the i^{th} pixel in the intercepted watermarked image "WI"
P_{Wi} is then converted to binary and the hamming code is calculated for its 4 MSBs to obtain T.
$\Rightarrow (102)_{10} = (01100110)_2$
$\Rightarrow c = H_{(4,7)}(0110) = 0110011 \Rightarrow T = (c_3, c_2, c_1) = (011)_2 = 3_{10}$.
2) Calculate $z = mod\ (P_{Wi}, 8) \Rightarrow z = mod(102, 8) = 6$.
This means that the z^{th} position in R contain the value of T.
$\Rightarrow R(6) = 3; \Rightarrow R = \{?, ?, ?, ?, ?, ?, 3, ?\}$
3) The list R is now constructed using equation 7.
$R((z+j)\,mod 8) = (W+j)\,mod 8 \quad where\, j = 0:7$
$\Rightarrow R(6) = 3; R(7) = 4, R(0) = 5; R(1) = 6; R(2) = 7; R(3) = 0; R(4) = 1; R(5) = 2$
$\Rightarrow R = \{5, 6, 7, 0, 1, 2, 3, 4\}$
4) The first element in the list R represents the value K_i where i is the index of the pixel in question : $K_i = 5$.
5) The i^{th} pixel could now be modified and the watermark substituted with the possession of the list R.

B. Online Attack

The second approach to attack the scheme under study is to use one of the online attacks. Online attacks could be summarized in three main approaches [39]:

1) **KPA** Known plaintext attack : In this scenario the cryptanalyst has one or several plain-text and their corresponding cipher-text. the cryptanalyst then tries to conclude the key or an equivalent key from the analysis of these pairs.
2) **CPA** Chosen plain-text attack: As in the case of KPA the cryptanalyst possesses pairs of plain-text and their corresponding ciphers only in this scenario, the attacker has access to the encryption machinery and can chose the plain-texts to be encrypted.
3) **CCA** Chosen cipher-text attack : In this scenario the attacker has access to the decryption machinery and can chose cipher-texts to get the corresponding plain-texts. Based on the study of these plain/cipher-texts the cryptanalyst tries to conclude the key or an equivalent of the key.

These scenarios represent the most common techniques in cryptanalysis. any security system should be tested to avoid vulnerability against these attacks.

Using KPA or CPA, only a single pair of original image and its corresponding watermarked image is needed to break the system and reveal the secret keys (The list R for each pixel and the list K for the image):

Let "OI" be the original image and "WI" its corresponding watermarked image with size $M \times N$, and OP_i, WP_i are the pixels of "OI" and "WI" respectively, where i represents the index of the pixel, the secret lists R and K could be calculated as follows:

1) Find $z = mod\,(OP_i, 8)$, then calculate the list PR, where $PR = \{P_i - z + t\ ;\ t = 0, 1, 2..., 7\}$.
2) Convert OP_i (or WP_i) to binary and and calculate the hamming code for its 4 MSBs : $c = (c_7, c_6, c_5, c_4, c_3, c_2, c_1)$. The value T is the integer value of $W = (c_3, c_2, c_1)$
3) Find the value of WP_i in the list PR and save its index as j.
4) j represents the position of T in the list R, so the list R could now be calculated using equation 8

$$R((j+t)\,mod 8) = (T+t)\,mod 8 \quad where\, t = 0:7. \tag{8}$$

5) The first element in the list R represents the secret value K_i. Once all pixel are processed the list K will be revealed.

With the revelation of the secret list K the image could be manipulated and the watermark is successfully replaced without being detected by the extraction scheme.

a numerical example is presented next :

a) Example:: In this example the original value of the pixel $OP_i = 165$ and its corresponding watermarked pixel $WP_i = 167$.

1) Calculate $z = mod\ (OP_i, 8) \Rightarrow z = mod(165, 8) = 5$.
Calculate list PR, where $PR = \{P_i - z + t\ ;\ t = 0, 1, 2..., 7\}$.
$\Rightarrow PR = \{160, 161, 162, 163, 164, 165, 166, 167\}$.
2) OP_i is converted to binary and the hamming code c for its 4 MSBs is calculated:

$\Rightarrow (165)_{10} = (10100101)_2$
$\Rightarrow c = H_{(4,7)}(1010) = 1010010 \Rightarrow T = (c_3, c_2, c_1) = (010)_2 = 2_{10}$.

3) Search for WP_i in the list PR. $\Rightarrow$ 167 in the 7^{th} position. $\Rightarrow j = 7$.
4) $R(j) = T \Rightarrow R(7) = 2$,$\Rightarrow R(7) = 2; \Rightarrow R = \{?, ?, ?, ?, ?, ?, ?, 2\}$
Starting from the position $j = 7$ the list R is revealed using equation 8.
$R((j+t) \, mod \, 8) = (T+t) \, mod \, 8 \quad where \, t = 0 : 7.$
$\Rightarrow R(7) = 2; R(0) = 3; R(1) = 4; R(2) = 5; R(3) = 6; R(4) = 7; R(5) = 0; R(6) = 1$
$\Rightarrow R = \{3, 4, 5, 6, 7, 0, 1, 2\}$
5) The first element in R represents the i^{th} element in the secret list K: $K_i = R(0) = 3$.

Fig. 3 shows the results of the attack. Multiples images were used in the experiments, we were able to calculate the keys used in the embedding process, as a result, the watermarks were successfully removed in order to manipulate the images, then using the calculated keys, new watermark are embedded into the falsified images in order to prevent any alarms in the extraction process.

The experiments shows that the extraction scheme failed to detect the falsifications which proves the weakness of the proposed scheme.

IV. Conclusion

In this paper, a cryptanalysis of a recently proposed watermarking scheme is conducted, two types of attacks were conducted successfully. As a result, the watermarked images could be falsified without triggering any alarm in the extraction process. This proves that even if very complicated steps were used in the design of a cryptographic scheme, that doesn't mean that the scheme is secure, several cryptalysis techniques could be used to attack these scheme, and these cryptanalysis techniques should be taken into consideration when designing a cryptographic scheme. As future work, an improvement of the attacked scheme could be proposed to cover the flaws and problems demonstrated in this paper.

Acknowledgment

The authors would like to thank the deanship of research at the Islamic University of Madinah, Kingdom of Saudi Arabia for supporting this research.

References

[1] S. Prasad and A. K. Pal, "Hamming code and logistic-map based pixel-level active forgery detection scheme using fragile watermarking," *Multimedia Tools and Applications*, Apr 2020. [Online]. Available: https://doi.org/10.1007/s11042-020-08715-x

[2] N. Sivasubramanian and G. Konganathan, "A novel semi fragile watermarking technique for tamper detection and recovery using iwt and dct," *Computing*, 2020.

[3] O. Evsutin and K. Dzhanashia, "Watermarking schemes for digital images: Robustness overview," *Signal Processing: Image Communication*, vol. 100, p. 116523, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0923596521002551

[4] W. H. Alshoura, Z. Zainol, J. S. Teh, and M. Alawida, "An fpp-resistant svd-based image watermarking scheme based on chaotic control," *Alexandria Engineering Journal*, vol. 61, no. 7, pp. 5713–5734, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110016821007213

[5] M. Swain and D. Swain, "An effective watermarking technique using btc and svd for image authentication and quality recovery," *Integration*, vol. 83, pp. 12–23, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167926021001255

[6] S. O. V. Aslantas and S. Ozturk, "Improving the performance of dct-based fragile watermarking using intelligent optimization algorithms," *Opt Commun*, vol. 282, pp. 2806–2817, 2009.

[7] G. Bhatnagar and B. Raman, "A new robust reference logo watermarking scheme," *Multimedia Tools Appl*, vol. 52, pp. 621–640, 2011.

[8] Y. Y. P.P. Niu, X.Y. Wang and M. Lu, "A novel color image watermarking scheme in nonsampled contourlet-domain," *Expert Syst Appl*, vol. 38, pp. 2081–2098, 2011.

[9] C.-Y. Lin and S.-F. Chang, "Sari: Self-authentication-and-recovery image watermarking system," *ACM Multimedia*, vol. Ottawa, Canada, Sep. 30 - Oct 5, 2001.

[10] T.-Y. Lee. and S. D. Lin, "Dual watermark for image tamper detection and recovery," *Pattern Recognition*, vol. 41, pp. 3497–3506, 2008.

[11] S. Poonkuntran and R. S. Rajesh, "Chaotic model based semi fragile watermarking using integer transforms for digital fundus image authentication," *Multimed Tools Appl*, vol. DOI 10.1007/s11042-012-1227-5, 2012.

[12] H. H. Yaoran Huo and F. Chen, "A semi-fragile image watermarking algorithm with two-stage detection," *Multimed Tools Appl*, vol. DOI 10.1007/s11042-012-1317-4, 2013.

[13] T. Luo, G. Jiang, X. Wang, M. Yu, F. Shao, and Z. Peng, "Stereo image watermarking scheme for authentication with self-recovery capability using inter-view reference sharing," *Multimed Tools Appl*, vol. DOI 10.1007/s11042-013-1435-7, 2013.

[14] S.-J. Horng, M. Farfoura, P. Fan, X. Wang, T. Li, and J.-M. Guo, "A low cost fragile watermarking scheme in h.264/avc compressed domain," *Multimedia Tools and Applications*, vol. 72, pp. 2469–2495, 2014.

[15] S.-J. Horng, D. Rosiyadi, P. Fan, X. Wang, and M. Khan, "An adaptive watermarking scheme for e-government document images," *Multimedia Tools and Applications*, vol. 72, pp. 3085–3103, 2014.

[16] S.-J. Horng, D. Rosiyadi, T. Li, T. Takao, M. Guo, and M. K. Khan, "A blind image copyright protection scheme for e-government," *Journal of Visual Communication and Image Representation*, vol. 24, pp. 1099 – 1105, 2013.

[17] D. Rosiyadi, S.-J. Horng, P. Fan, X. Wang, M. Khan, and Y. Pan, "Copyright protection for e-government document images," *MultiMedia, IEEE*, vol. 19, pp. 62–73, 2012.

[18] O. Benrhouma, H. Hermassi, and S. Belghith, "Tamper detection and self-recovery scheme by dwt watermarking," *Nonlinear Dynamics*, vol. 79, no. 3, pp. 1817–1833, 2015. [Online]. Available: http://dx.doi.org/10.1007/s11071-014-1777-3

[19] O. Benrhouma, H. Hermassi, A. A. Abd El-Latif, and S. Belghith, "Chaotic watermark for blind forgery detection in images," *Multimedia Tools and Applications*, pp. 1–24, 2015. [Online]. Available: http://dx.doi.org/10.1007/s11042-015-2786-z

[20] W. Lu, H. Lu, and F. Chung, "Robust digital image watermarking based on sub-sampling." *Applied Mathematics and computation*, vol. 181, pp. 886–893, 2006.

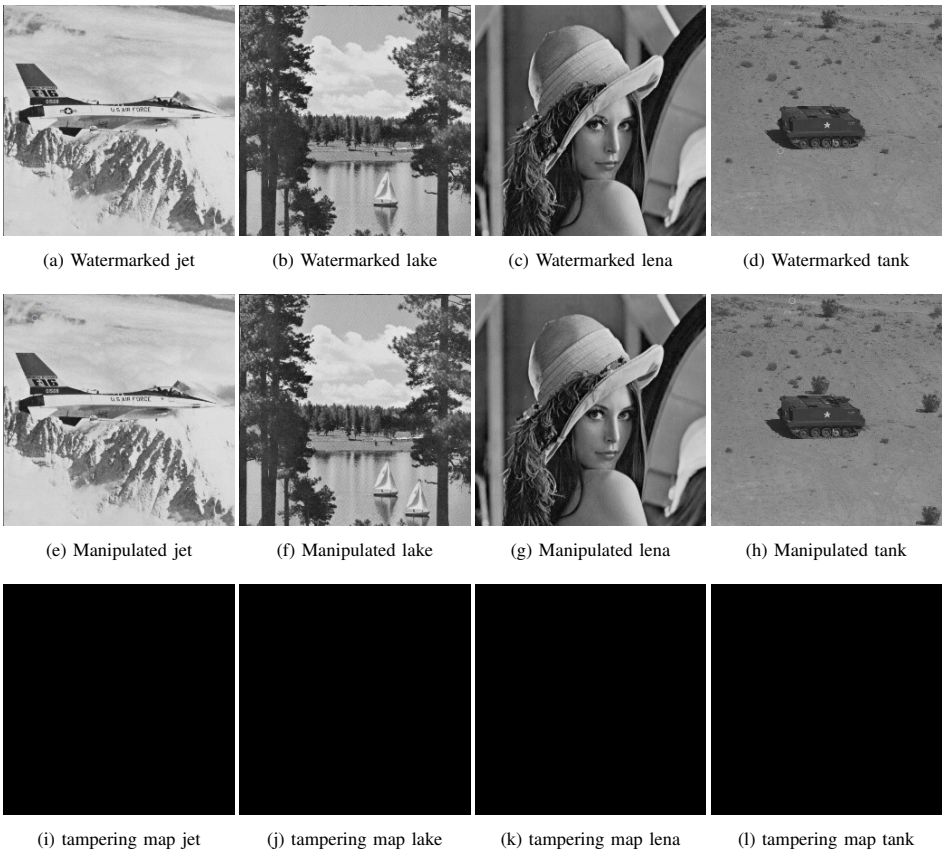
[21] D. Simitopoulos, D. Koutsonanos, and M. Strintzis, "Robust image watermarking based on generalized radon transformations." *IEEE Transctions on Circuits and Systems for Video Technology.*, vol. 13, pp. 732–745, 2003.

[22] H. Tang, C.W. Hang, "A feature-based robust digital image watermaking shceme." *IEEE Transctions on Signal Processing.*, vol. 51, pp. 950–958, 2003.

[23] M. Celik, G. Sharmar, and A. Tekalp, "Hierarchical watermarking for secure image authentication with localization." *IEEE Transctions on Image Processing.*, vol. 11, pp. 585–594, 2002.

[24] E. chang, M. Kankanhalli, X. Guan, Z. Huang, and Y. Wu, "Robust image authentication using content based compression." *ACM Multimedia System Journal*, vol. 2, pp. 121–130, 2003.

[25] J. Fridrich, M. Goljan, and A. Baldoza, "New fragile authentication watermarks for image." *Proceeding of IEEE International Conference on Image Processing.*, vol. 1, pp. 446–449, 2000.



(a) Watermarked jet (b) Watermarked lake (c) Watermarked lena (d) Watermarked tank

(e) Manipulated jet (f) Manipulated lake (g) Manipulated lena (h) Manipulated tank

(i) tampering map jet (j) tampering map lake (k) tampering map lena (l) tampering map tank

Fig. 3. Results of the Attack: Tampered Images and the Corresponding Tampering Map

[26] C. Lin and S. Chang, "A robust image authentication method distinguishing jpeg compression from malicious manipulation." *IEEE Transctions on Circuits and Systems for Video Technology.*, vol. 11, pp. 153–168, 2001.

[27] A. Paquet, R. Ward, and I. Pitas, "Wavelet packets-based digital watermaking for image verification and authentication." *Signal Processing.*, vol. 183, pp. 2117–2132, 2003.

[28] N. Wong, P. Memon, "Secret and public key authentication watermarking schemes that resist vector quantization attack." *Proceeding ofSPIE on Security and Watermarking of Multimedia Contents.*, vol. 3971, pp. 417–427, 2000.

[29] F. Yeung, M. Mintzer, "An invisible watermarking technique for image verification." *Proceeding of IEEE International Conference on Image Processing.*, vol. 2, pp. 680–683, 1997.

[30] J. Fridrich, "Security of fragile authentication watermaks with localization." *Proceeding ofSPIE on Security and Watermarking of Multimedia Contents.*, vol. 4675, pp. 691–700, 2002.

[31] B. B. Haghighi, A. H. Taherinia, and A. H. Mohajerzadeh, "Trlg: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using lwt and ga," *Information Sciences*, vol. 486, pp. 204 – 230, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025519301707

[32] J. Molina-Garcia, B. P. Garcia-Salgado, V. Ponomaryov, R. Reyes-Reyes, S. Sadovnychiy, and C. Cruz-Ramos, "An effective fragile watermarking scheme for color image tampering detection and self-recovery," *Signal Processing: Image Communication*, vol. 81, p. 115725, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0923596519306897

[33] L. Teng, X. Wang, and X. Wang, "Cryptanalysis and improvement of a chaotic system based fragile watermarking scheme," {*AEU*} - *International Journal of Electronics and Communications*, vol. 67, no. 6, pp. 540 – 547, 2013.

[34] M. Botta, D. Cavagnino, and V. Pomponiu, "A successful attack and revision of a chaotic system based fragile watermarking scheme for image tamper detection," {*AEU*} - *International Journal of Electronics and Communications*, vol. 69, no. 1, pp. 242 – 245, 2015.

[35] M. Li, J. Zhang, and W. Wen, "Cryptanalysis and improvement of a binary watermark-based copyright protection scheme for remote sensing images," *Optik - International Journal for Light and Electron Optics*, vol. 125, no. 24, pp. 7231 – 7234, 2014.

[36] O. Benrhouma, H. Hermassi, and S. Belghith, "Security analysis and improvement of an active watermarking system for image tampering detection using a self-recovery scheme," *Multimedia Tools and Applications*, pp. 1–24, 2016.

[37] H. He and J. Zhang, "Cryptanalysis on majority-voting based self-recovery watermarking scheme," *Telecommun Syst*, vol. 49, pp. 231–238, 2012.

[38] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, vol. 9, pp. 5–38, 1883.

[39] D. A. Guardeno, "Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems," Ph.D. dissertation, Escuela Técnica Superior de Ingenieros Agronomos, Universidad Politécnica de Madrid, 2009.