IJEMD-CSAI, 1 (1) (2022), 30 - 40 https://doi.org/10.54938/ijemdcsai.2022.01.1.33

International Journal of Emerging Multidiciplinaries:

Computer Science & Artificial Intelligence

Research Paper

Journal Homepage: www.ijemd.com

ISSN (print): 2791-0164

IJEMD | International Journal of Emerging Multidisciplinaries
COMPUTER SCIENCE & ARTIFICIAL INTELLIGENCE

An NGram-based Copyright Protection for Digital Images

Azzam Sleit[1] **and Adel Abusitta**[2*]

[1]*KINDI Center for Computing Research, Doha, Qatar; Department of Computer Science, University of Jordan, Amman, Jordan*
[2]*School of Information Studies, McGill University, Montreal, Canada*
[*]*Corresponding author*

Abstract

This paper introduces an NGram-based approach for digital images copyright protection. The advantage of the proposed approach compared to the existing works, is that it does not always require the whole elements (e.g., bits) of the watermark pattern to be embedded into the original digital image. This, in turn, allows us to protect the digital images while at the same time minimizing the chances of having low quality marked digital images. The best case occurs when no element of the pattern is embedded into the original digital image. In contrast, the worst case, which rarely happens, occurs when all elements are embedded into the digital image. Moreover, the use of an NGram approach allows us to efficiently and easily reach any part of the image using the corresponding level numbers and addresses. This makes it more efficient especially for complex and high-dimensional data (e.g., images and videos). Experimental results show the effectiveness of the proposed approach in terms of the ability to recover the watermark pattern from the marked digital image even if major changes are applied to the original digital image.

Keywords: *image watermark; NGram; serial NGram; copyright protection; image processing.*

1. Introduction

The proliferation of both digitized images and advanced image-processing applications has made the modification and duplication of images much easier than before. Therefore, it is becoming increasingly important to have advanced watermarking technologies for copyright protection of digital images [10] [14] [7]. Technically speaking, if someone is looking to protect her digital image, she has to register the image with the trusted Copyright Office (CO). This however, can be done by submitting a copy to them. The CO archives the digital image, along with information about the rightful owner. When dispute occurs, the owner contacts the CO to obtain proof that she is the rightful owner [23] [6] [24]. If the owner's digital image was not registered, then at least, the owner should be able to provide the film negative. However, with the rapid and increased acceptance of digital photography, the film negative might not be available.

Digital watermarking can be considered as the process of embedding or hiding Identification Information (IF) into digital data such as images and videos, in order to prevent attackers illegally use the protected data without getting the acceptance of the owner [25][17][5]. In particular, the IF is called a Watermark Pattern (WP) and the original digital image, after embedding the pattern, is called a Marked Image (MI). In fact, this process takes place by changing the contents of the digital image [5]. Moreover, a secret key is used, in order to guide us on how to hide the WP into the image to produce the MI. Fig. 1.1 shows the schema of the digital watermarking.

The problem of the existing watermarking approaches is that they work on improving hiding algorithms to produce robust marked images. Two disadvantages are associated in these approaches: 1) the protection cannot be achieved without affecting the quality of the protected images. In other words, the protection is obtained on the account of the quality; 2) when the protecting algorithm is applied on big and high-dimensional data (e.g., images), the time needed for the protection and verification largely increases.

Email addresses: **azzam.sleit@ju.edu.jo (A. Sleit), adel.abusitta@mcgill.ca (A. Abusitta)**

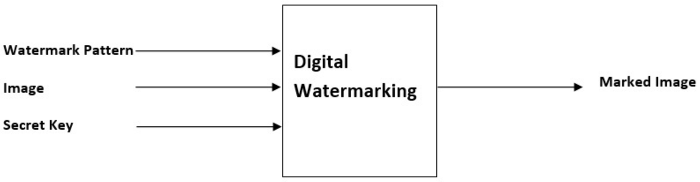


Figure 1.1: Watermarking.

To address the above-mentioned shortcomings, we propose an NGram-based approach for digital image copyright protection. The proposed method does not always require the whole bits of the watermark pattern to be embedded into the images. This enables us to protect the digital images while at the same time minimizing the chances of having low-quality marked digital images. The best case occurs when no bit in the pattern is embedded into the original digital image. In contrast, the worst case, which rarely happens, occurs when all bits are embedded into the digital image. The proposed method allows us to efficiently reach any part of the image using the corresponding level numbers and addresses. This, in turn, makes it more efficient, especially for high-dimensional data such as images and videos. Our results show the effectiveness of the proposed approach, compared to the existing approaches, in terms of the ability to recover the watermark pattern from the marked digital image even if major changes are applied to the original digital image.

The rest of this paper is organized as follows. Section 2 reviews some previous work. Section 3 briefly discusses the NGram transform while Section 4 explains the proposed watermark method. Section 5 shows the experimental results. Finally, Section 6 concludes the paper.

2. Related Work

There are many works propose different approaches for digital watermarking [10] [14] [7] [5] [9]. In fact, digital watermarking can be classified into the following three types: embedding-based, non-embedding-based and semi-embedding-based approaches [13] [11] [15] [4] [18] [12] [1] [19] (Fig. 2.1). The embedding-based approach is a classical approach used to embed all pattern's bits into the original image. The non-embedding-based approach is a new concept defined in [10] [2], which is based on visual cryptography [14] and does not require the watermark pattern to be embedded into the original digital images. Instead, verification information is generated, which is used to verify the ownership of the digital image [10] [14] [20] [3]. Finally, the semi-embedding-based approach is a combination between the embedding-based and non-embedding-based approach. In particular, this approach (proposed in this paper) has the advantage that there is no need to embed all the pattern's bits into the original image. This, in turns, allows us to protect digital images while at the same time minimizing the chances of having low-quality marked digital images [21] [22].

Sleit and Abusitta [19] propose a visual cryptography based digital image copyright protection. The proposed framework is based on visual cryptography defined by Noor and Shamir [14]. They propose to select random data points from the original data rather than specific data points. Their method has an advantage that it does not require the watermark pattern to be embedded into the original data. To this end, verification data is produced which can be adopted to verify who owns the digital data. Similarly, other works (e.g., [8], [10]) present an improved approach based on Visual Cryptography. The techniques used also do not need to embed the pattern into the original image. Instead, verification information is used to prove the ownership of the group of digital images.

Recently, Abusitta [1] proposes a new method based on the relationship between randomly selected pixels and their 8-neighbors' pixels. This relationship keeps the marked image coherent against diverse attacks even if the most significant bits of randomly selected pixels have been modified.

Our method is close to [10], which is based on visual cryptography [14]. The method proposed in [10] is based on the simple (2, 2) visual threshold scheme proposed by Naor and Shamir [14]. In this technique, the owner of the digital image has to choose w(pattern's weight) * l (pattern's length) black/white image as a watermark pattern Pt and a secret key K. Then, VI (Verification Information) is created from the original digital image $N * 1$ IM and the pattern Pt using the secret key K; as the following steps:

Step 1: Make the secret key K as the starting point (i.e., seed) to create $w * l$ different random numbers over the interval $[0, N * 1]$.

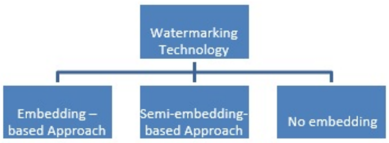
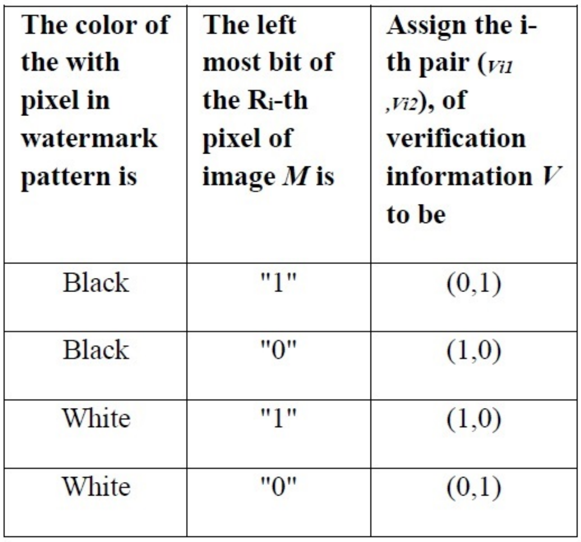


Figure 2.1: Digital watermarking classifications.

Step 2: Assign the i-th pair (VI_{i1}, VI_{i2}) of the VI, according to the instructions given in Fig. 2.2.



The color of the with pixel in watermark pattern is	The left most bit of the R_i-th pixel of image M is	Assign the i-th pair (v_{i1} ,v_{i2}), of verification information V to be
Black	"1"	(0,1)
Black	"0"	(1,0)
White	"1"	(1,0)
White	"0"	(0,1)

Figure 2.2: Rules for assigning values of VI.

Step 3: Aggregate all the (VI_{i1}, VI_{i2}) pairs to build the VI. The VI should be given to the trustworthy neutral organization (TNO).
if the owner would like to claim that an image *IM*’ is a copy of *IM* (i.e., the original digital image), she should provide the key K to the TNO, and the pattern *Pt* is restored using *IM*’ and VI as the following steps:

1. Use K as the starting point (i.e., seed) to create $w*l$ different random numbers over the interval [0, $N*1$].

2. The color of the i-th pixel of the pattern *Pt*’ will be assigned based on *IM*’ as follows:

1. Obtain the left-most bit, *bit*, of the Ri-th pixel of *IM*’, and if *bit* is 0 then, assign VI_i= (0,1); otherwise assign VI_i = (1,0).

2. If VI_i is equal to the i-th pair of VI then assign the color ’white’ to the i-th pixel of *Pt*’; otherwise, assign the color ’black’ to the i-th pixel of *Pt*’.

3. If *Pt*’ can be known and recognized as *Pt*, the TNO will define that *IM*’ is a copy of *IM*.

The above-mentioned method is not robust against several changes applied to images: illumination, rotation, distortion, and image scaling. Fig. 2.3 shows some results.
In Section 4, we present the proposed method to address the above-mentioned deficiencies.

2.1. The NGram Transform

The NGram transform is a function defined by [16]. It starts with a stream of tokens as can be seen in Fig. 2.4. In Fig. 2.4, every two pixels from an image is treated as a token. These are combined in pairs to produce new tokens. Each new token is “learned” – stored in a list or lookup table. If the token has been seen before,

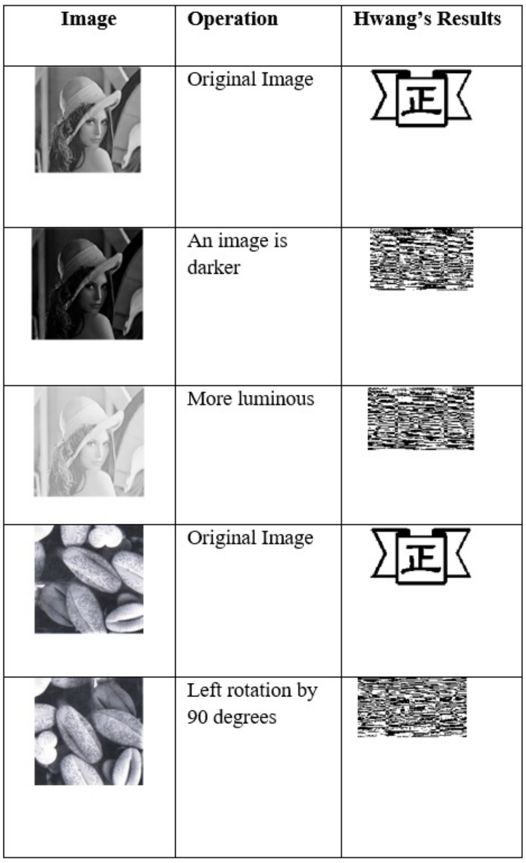


Image	Operation	Hwang's Results
	Original Image	
	An image is darker	
	More luminous	
	Original Image	
	Left rotation by 90 degrees	

Figure 2.3: Results of Hwang's work

its count is incremented; otherwise the token is added with a count of one. For each token pair input, a single token is output, representing the "address" or name of the token pair in the list. Thus, at the first, or lowest level, the pixel pair "001100" becomes "A", the name of the list entry that stored the "001100" token. The next pixel pair, "110010" becomes "B", etc. The resulting output stream, "ABCDEFGDHDIJ…" is processed the same way, creating a level 2 list and a new output stream. This process is repeated until a single token result.

The original input token stream can be recalled from a result token/level pair. Starting with the "A" token at level 6, look up the A entry in the level 6 dictionary. The result is "AB". Look up each of the "A" and "B" in the level 5 dictionary, resulting in "AB" and "CD". Look up each of the "A", "B", "C" and "D" in the level 4 dictionary, resulting in "AB", "CD" , "EF" and "GH" . Continue this process through level 1, resulting in the original input tokens. Any part of an image can be reached using the level and address. For example the first four pixels of an image are reached by using "A 2", which means level "A" and address 1.

3. The proposed method

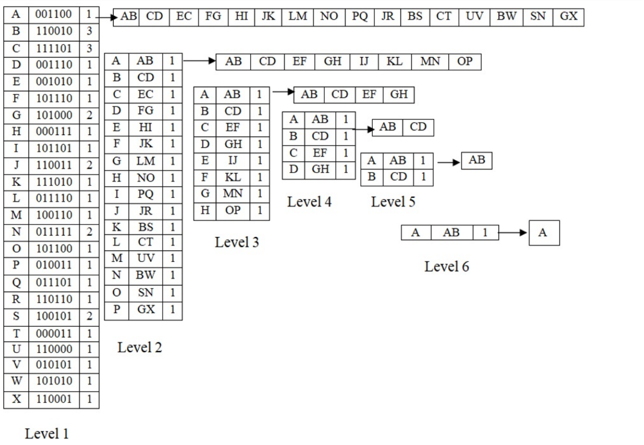
To illustrate the proposed method, we introduce the following example. Assume that we have an image like the one in Fig. 3.1, and we would like to mark it using the pattern in Fig. 3.2. The proposed method works as the following steps:

A. Key Generation

The owner should select 11 (number of bits in the pattern) even numbers randomly. The summation of these numbers equals to Image Height (H) * Image Width (W), if the total number of pixels in the image is even, and equals to (H * W)-1, if the total number of pixels in is odd. In this example, we have 8 * 8 = 64 pixels. Assume the owner has selected the following numbers: 4, 10, 2, 10, 6, 4, 4, 2, 4, 8, 10.

B. Selection Process

We divide the image (Fig. 3.1) based on the selected numbers in the previous step. Fig. 3.3 shows the image after the division has been applied. Note that in Fig. 3.3, each part of the image can be reached from the level number and address using the NGram Transform presented in Section 3.



A	001100	1
B	110010	3
C	111101	3
D	001110	1
E	001010	1
F	101110	1
G	101000	2
H	000111	1
I	101101	1
J	110011	2
K	111010	1
L	011110	1
M	100110	1
N	011111	2
O	101100	1
P	010011	1
Q	011101	1
R	110110	1
S	100101	2
T	000011	1
U	110000	1
V	010101	1
W	101010	1
X	110001	1

AB	CD	EC	FG	HI	JK	LM	NO	PQ	JR	BS	CT	UV	BW	SN	GX

Level 1

A	AB	1
B	CD	1
C	EC	1
D	FG	1
E	HI	1
F	JK	1
G	LM	1
H	NO	1
I	PQ	1
J	JR	1
K	BS	1
L	CT	1
M	UV	1
N	BW	1
O	SN	1
P	GX	1

AB	CD	EF	GH	IJ	KL	MN	OP

Level 2

A	AB	1
B	CD	1
C	EF	1
D	GH	1
E	IJ	1
F	KL	1
G	MN	1
H	OP	1

AB	CD	EF	GH

Level 3

A	AB	1
B	CD	1
C	EF	1
D	GH	1

AB	CD

Level 4

A	AB	1
B	CD	1

AB

Level 5

A	AB	1

A

Level 6

Figure 2.4: An NGram of an image.

001	100	110	010	111	101	001	110
001	010	111	101	101	110	101	000
000	111	101	101	110	011	111	010
011	110	100	110	011	111	101	100
010	011	011	101	110	011	110	110
110	010	100	101	111	101	000	011
110	000	010	101	110	010	101	010
100	101	011	111	101	000	110	001

Figure 3.1: Image.

0	1	0	1	0	1	0	0	1	0	1

Figure 3.2: Pattern.

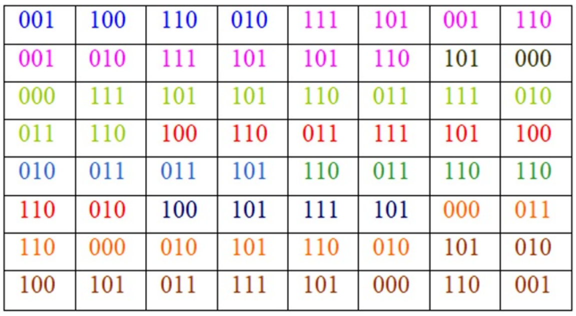
Thereafter, the owner should select 11 different numbers from 1 to 11 randomly; each number represents a specific part of the image. For example, 5 represents part 5, 2 represents part 2 and so on. Assume that the owner has selected the following numbers (5, 2, 1, 10, 3, 6, 4, 8, 9, 7, 11), and these numbers represent (part 5, part 2, part 1, part 10, part 3, part 6, part 4, part 8, part 9, part 7, part 11), respectively.

D. Hiding process

In this process, each bit in the pattern (Fig. 3.2) should be hidden in one part. In our example, the first bit will be hidden in part 5, the second bit in part 2, the third bit in part 1, and so on.
The hiding process is applied from the most significant bit to the least significant bit. The following example illustrates the proposed hiding algorithm. Assume that we want to hide the first bit of the pattern in Fig. 3.2. The value of this bit is 0, therefore it will be hidden in part 5 by XORing all pixels in part 5 and looking firstly at the most significant bit on the result. If the value is 0, the bit will be considered as already hidden. Otherwise, if the value is 1, then we move to the left. If the value is 0, the bit will be considered as already hidden. Otherwise, if the value is 1, then we move to the left, if the value is 0, the bit will be considered as already hidden. Otherwise, if the value is 1, the last bit in the last pixel (in part 5) will be changed.
So, in our example, we have 100 XOR 110 XOR 011 XOR 111 XOR 101 XOR 100 = 111, in part 5. Since there is no 0 in 111, we change the last bit in the last pixel (in part 5), as shown in Fig. 3.4.

After hiding all bits of the pattern in the image, a new image will be generated, as can be seen in Fig. 3.4.

Then, we apply the NGram transform on the generated image, as shown in Fig. 3.5.

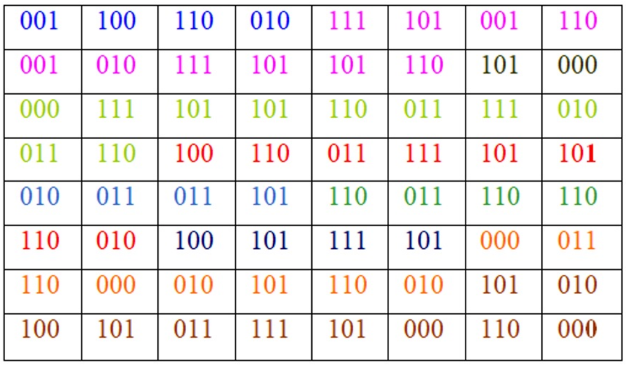


001	100	110	010	111	101	001	110
001	010	111	101	101	110	101	000
000	111	101	101	110	011	111	010
011	110	100	110	011	111	101	100
010	011	011	101	110	011	110	110
110	010	100	101	111	101	000	011
110	000	010	101	110	010	101	010
100	101	011	111	101	000	110	001

Figure 3.3: After applying division.

The serial NGram of the image (Fig. 3.5) is used to generate the Verification Information (VI) as shown in Fig. 3.6. The VI is then used as a key to retrieve the pattern. This key is described as follows: M1 H2 3 ; B2 C2 F1 1 ; A2 1 ; T1 M2 B1 1 ; G1 2 ; I2 1 ; C3 L1 1 ; B1 2 ; S1 C1 2 ; J2 2 ; W1 H3 3.

D. Verification.
The owner sends the marked image, serial NGram (Fig. 3.5) and check-sum to the neutral organization.



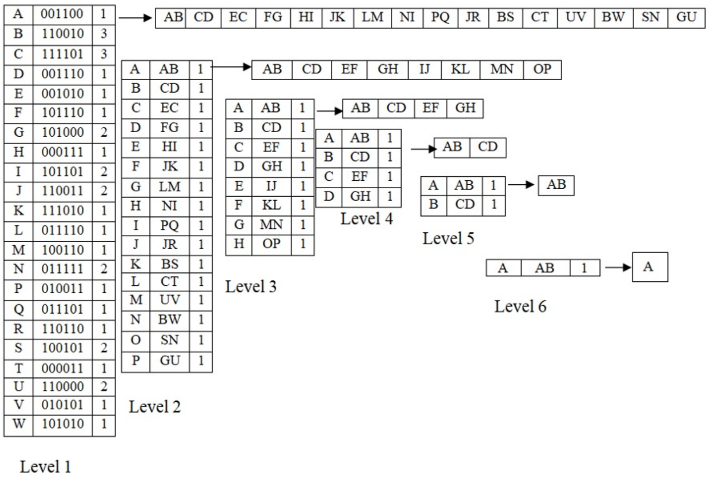
001	100	110	010	111	101	001	110
001	010	111	101	101	110	101	000
000	111	101	101	110	011	111	010
011	110	100	110	011	111	101	101
010	011	011	101	110	011	110	110
110	010	100	101	111	101	000	011
110	000	010	101	110	010	101	010
100	101	011	111	101	000	110	000

Figure 3.4: Output after hiding the pattern.

If the owner wants to prove the ownership of some data F, a watermark pattern P' is generated from the image, the verification is done as follows:

- The owner gives the VI (Fig.3.6) to the TNO
- The TNO determines the check-sum of the VI and compares the result with the check-sum provided by the owner.
- If the calculated check-sum is equal to the received check-sum, the organization uses the VI to retrieve the pattern from the image.
- To retrieve the pattern, we need first to apply image rotation from 1 to 360 degree. For each degree, we set a counter to zero and compare each pixel in the registered image with the corresponding pixel in the rotated image; the counter is incremented by one, if there is a match between each two pixels. The output of this step is shown in 3.7, which presents the number of successful matches with respect to different degrees of image rotation.
- We select the rotated image that leads to the maximum number of matches in order to be used to extract the VI from it.

It is very obvious that the above two steps solve the problem of image rotation that might be applied by the attacker to mislead the proposed watermarking method. The pattern can be extracted from the image using the VI. For example, the first bit in the pattern can be extracted using the first part of the VI (M1 H2 3). This part means go to the address M at level 1 according to Fig. 3.7 (NGram), the result here is “100110”, then go to the address H at level 2, the result is “N I”, then look at “N” at level 1, the result is “011111” and look at “I” at level 1, the result is“101101”. The result is: 100 110 011 111 101 101. Finally, we XOR all those pixels (100 Xor 110 Xor 011 Xor 111 Xor 101 Xor 101) and look to the third bit in the result, which represents the first bit of the pattern.



A	001100	1
B	110010	3
C	111101	3
D	001110	1
E	001010	1
F	101110	1
G	101000	2
H	000111	1
I	101101	2
J	110011	2
K	111010	1
L	011110	1
M	100110	1
N	011111	2
P	010011	1
Q	011101	1
R	110110	1
S	100101	2
T	000011	1
U	110000	2
V	010101	1
W	101010	1

AB	CD	EC	FG	HI	JK	LM	NI	PQ	JR	BS	CT	UV	BW	SN	GU

Level 1

A	AB	1
B	CD	1
C	EC	1
D	FG	1
E	HI	1
F	JK	1
G	LM	1
H	NI	1
I	PQ	1
J	JR	1
K	BS	1
L	CT	1
M	UV	1
N	BW	1
O	SN	1
P	GU	1

AB	CD	EF	GH	IJ	KL	MN	OP

Level 2

A	AB	1
B	CD	1
C	EF	1
D	GH	1
E	IJ	1
F	KL	1
G	MN	1
H	OP	1

AB	CD	EF	GH

Level 3

A	AB	1
B	CD	1
C	EF	1
D	GH	1

AB	CD

Level 4

A	AB	1
B	CD	1

AB

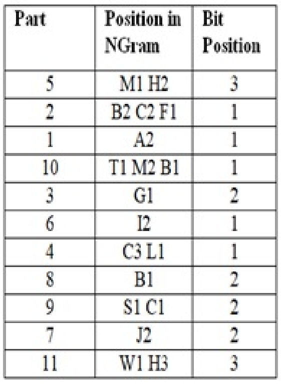
Level 5

A	AB	1

A

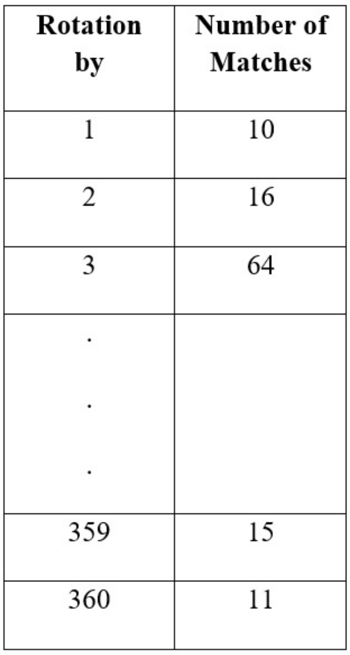
Level 6

Figure 3.5: The NGram of the marked image.



Part	Position in NGram	Bit Position
5	M1 H2	3
2	B2 C2 F1	1
1	A2	1
10	T1 M2 B1	1
3	G1	2
6	I2	1
4	C3 L1	1
8	B1	2
9	S1 C1	2
7	J2	2
11	W1 H3	3

Figure 3.6: Verification Information (VI).



Rotation by	Number of Matches
1	10
2	16
3	64
. . .	
359	15
360	11

Figure 3.7: Applying Rotations to the image

4. Experimental Results

We implemented the proposed approach in a 64-bit Windows 10 environment. The proposed method was studied on Lina, Beans, Moon images. The watermark pattern used is ”Cheng”. The size of ”Cheng” is 180 (width) x 97 (length). This pattern has been used in several works (e.g., [10], [19], [8],[1]). We tested the robustness of the proposed method against several changes applied to the images: illumination, rotation, distortion, scaling and combination between scaling and rotation. Figs. 4.1, 4.2 and 4.4 demonstrates that the watermark pattern can be recognized even when major changes were made to the original image.

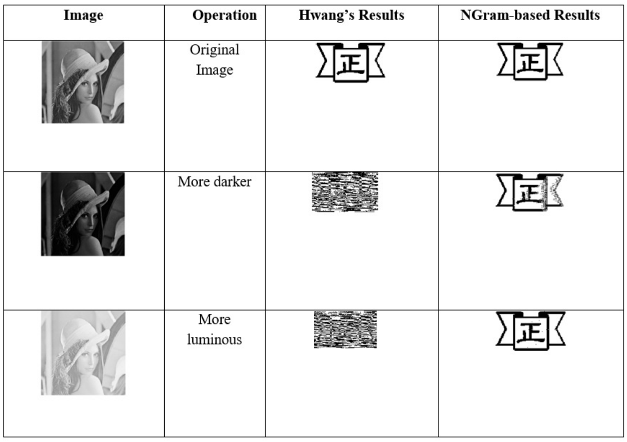


Image	Operation	Hwang's Results	NGram-based Results
	Original Image		
	More darker		
	More luminous		

Figure 4.1: Our results -Lina image (darker and luminous)

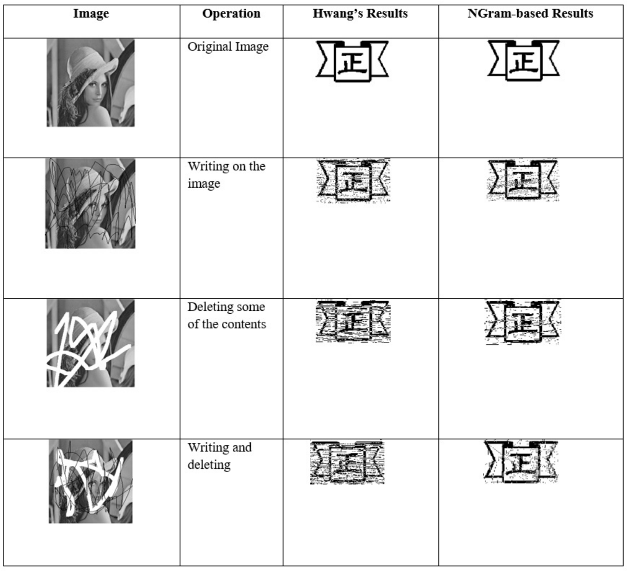


Image	Operation	Hwang's Results	NGram-based Results
	Original Image		
	Writing on the image		
	Deleting some of the contents		
	Writing and deleting		

Figure 4.2: Our results -Lina image (deleting and/or writing)

5. Conclusion

In this paper, we present an NGram-based approach for digital images copyright protection. The proposed approach does not always require the whole bits of the watermark pattern to be embedded into the original digital image. This enables us to protect the digital images while at the same time reducing the chances of having low-quality marked digital images. The best case occurs when no bit of the pattern is embedded into the original digital image. In contrast, the worst case, which rarely happens, occurs when all bits are embedded into the digital image. The NGram transform allows us to efficiently reach any part of the image using the corresponding level numbers and addresses. This makes it more powerful for complex and high-dimensional data such as images and videos. Our results show that the proposed method was able to

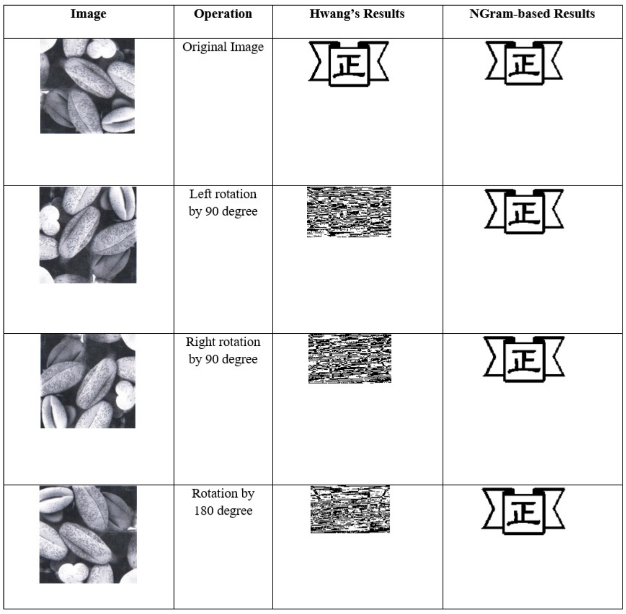


Image	Operation	Hwang's Results	NGram-based Results
	Original Image		
	Left rotation by 90 degree		
	Right rotation by 90 degree		
	Rotation by 180 degree		

Figure 4.3: Our results -Beans image (Rotation)

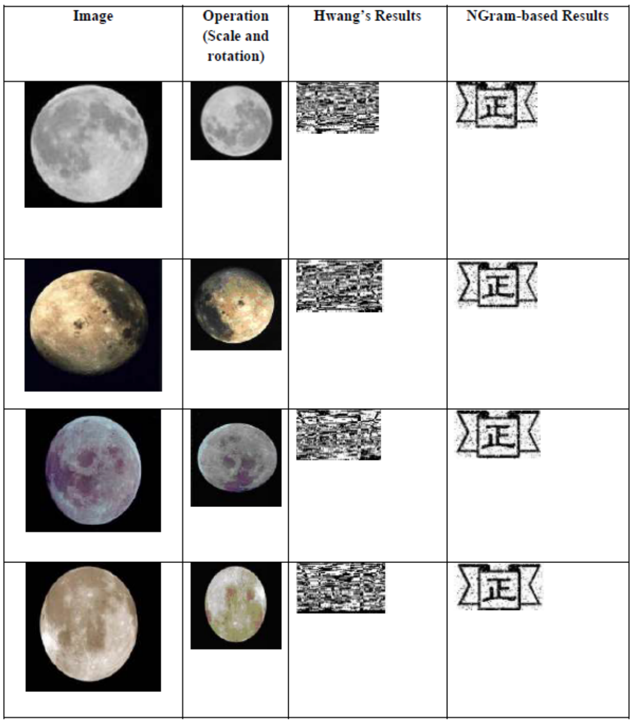


Image	Operation (Scale and rotation)	Hwang's Results	NGram-based Results

Figure 4.4: Our results -Moon (Scaling + Rotation)

recover the watermark pattern from the marked digital image even when major changes were made to the original digital image.

References

[1] Adel Hammad Abusitta. A visual cryptography based digital image copyright protection. 2012.

[2] Hebatallah Khattab Ala'a Al-Shaikh, Ahmad Sharieh, and Azzam Sleit. Resource utilization in cloud computing as an optimization problem. *Resource*, 7(6), 2016.

[3] Wesam Almobaideen, Roba Al-Soub, and Azzam Sleit. Msdm: Maximally spatial disjoint multipath routing protocol for manet. *Communications and Network*, 2013, 2013.

[4] Meryem Benyoussef, Samira Mabtoul, Mohamed El Marraki, and Driss Aboutajdine. Mammograms multiple watermarking scheme based on visual cryptography. In *Proceedings of the Mediterranean Conference on Information & Communication Technologies 2015*, pages 445–453. Springer, 2016.

[5] Jae-Su Do. Embedding a signature to pictures under wavelet transformation. *Convergence Security Journal*, 7(1):83–89, 2007.

[6] Elham Etemad, Shadrokh Samavi, SM Reza Soroushmehr, Nader Karimi, Mohammad Etemad, Shahram Shirani, and Kayvan Najarian. Robust image watermarking scheme using bit-plane of hadamard coefficients. *Multimedia Tools and Applications*, 77(2):2033–2055, 2018.

[7] Behrouz A Forouzan. *Cryptography & network security*. McGraw-Hill, Inc., 2007.

[8] Mahmoud A Hassan and Mohammed A Khalili. Self watermarking based on visual cryptography. In *Proceedings of World Academy of Science, Engineering and Technology*, volume 8, pages 159–162, 2005.

[9] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang. A watermarking technique based on one-way hash functions. *IEEE Transactions on Consumer Electronics*, 45(2):286–294, 1999.

[10] Ren-Junn Hwang. A digital image copyright protection scheme based on visual cryptography. *Tamkang Journal of science and Engineering*, 3(2):97–106, 2000.

[11] Pranesh Kulkarni and Girish Kulkarni. Visual cryptography based grayscale image watermarking in dwt domain. In *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pages 1443–1446. IEEE, 2018.

[12] Mbarek Marwan, Ali Kartit, and Hassan Ouahmane. Protecting medical images in cloud using visual cryptography scheme. In *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, pages 1–6. IEEE, 2017.

[13] Benyoussef Meryem and Mabtoul Samira. A short survey on image zero-watermarking techniques based on visual cryptography. In *2018 9th International Symposium on Signal, Image, Video and Communications (ISIVC)*, pages 157–162. IEEE, 2018.

[14] Moni Naor and Adi Shamir. Visual cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 1–12. Springer, 1994.

[15] Snehal Pawar. Extended capabilities of feature-extraction for digital image sharing by diverse image media. In *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, pages 1–6. IEEE, 2016.

[16] Maha Saadeh, Azzam Sleit, Mohammed Qatawneh, and Wesam Almobaideen. Authentication techniques for the internet of things: A survey. In *2016 cybersecurity and cyberforensics conference (CCC)*, pages 28–34. IEEE, 2016.

[17] Babloo Saha and Shuchi Sharma. Steganographic techniques of data hiding using digital images. *Defence Science Journal*, 62(1):11, 2012.

[18] Neha Shashni, Mainejar Yadav, et al. Cryptanalysis on digital image watermarking based on feature extraction and visual cryptography. In *Progress in Advanced Computing and Intelligent Engineering*, pages 425–435. Springer, 2019.

[19] Azzam Sleit and Adel Abusitta. A visual cryptography based watermark technology for individual and group images. *Systemics, Cybernetics and Informatics*, 5(2):24–32, 2008.

[20] Azzam Sleit, Mousa Al-Akhras, Inas Juma, and Marwah Alian. Applying ordinal association rules for cleansing data with missing values. *Journal of American Science*, 5(3):52–62, 2009.

[21] Azzam Sleit and Esam Al-Nsour. Corner-based splitting: An improved node splitting algorithm for r-tree. *Journal of information science*, 40(2):222–236, 2014.

[22] Azzam Sleit, Nada Misk, Fatima Badwan, and Tawfiq Khalil. Cloud computing challenges with emphasis on amazon ec2 and windows azure. *International Journal of Computer Networks & Communications*, 5(5):35, 2013.

[23] Chris Solomon and Toby Breckon. *Fundamentals of Digital Image Processing: A practical approach with examples in Matlab*. John Wiley & Sons, 2011.

[24] George Voyatzis and Ioannis Pitas. Applications of toral automorphisms in image watermarking. In *Proceedings of 3rd IEEE International Conference on Image Processing*, volume 2, pages 237–240. IEEE, 1996.

[25] Xiang-Gen Xia, Charles G Boncelet, and Gonzalo R Arce. A multiresolution watermark for digital images. In *Proceedings of international conference on image processing*, volume 1, pages 548–551. IEEE, 1997.