A Robust Digital Image Watermarking against Salt and Pepper using Sudoku

Shamsul Kamal Ahmad Khalid[1], Mustafa Mat Deris[1] and
Kamaruddin Malik Mohamad[1]
[1]Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia
86400 Parit Raja, Johor, Malaysia
shamsulk@uthm.edu.my, mmustafa@uthm.edu.my
malik@uthm.edu.my

ABSTRACT

Copyright information embedded in a digital data may disappear or become undetectable due to additive noise accidentally or deliberately introduced to a watermarked image. Several watermarking schemes have been proposed to overcome such attacks but remain inefficient due to its limited redundancy. In this paper, a new watermarking scheme that is robust against Salt and Pepper attack using Sudoku is proposed. It is based on Sudoku's permutation property that provide tightly related, redundant copies of watermark pieces distributed to all parts of the cover image. Using the classic 9X9 Sudoku puzzle and standard images, the proposed scheme has been implemented and tested with 24000 random Salt and Pepper attacks. The result indicates a positive capability to sustain attacks at close to 80% noise density.

KEYWORDS

watermarking; Sudoku; Salt and Pepper; redundant embedding; data hiding

1 INTRODUCTION

The growth of mobile computing, communication platforms and the availability of high speed broadband have contributed to the tremendous growth of digital data transmitted over the Internet. Digital products like pictures, movie or drama and flight boarding passes are now delivered via Internet. With powerful computing, unauthorized operations such as digital copying, tampering and removal of these data can be performed relatively easy. Due to such development, the protection of digital content has become increasingly important issue for content owners and service providers. Digital watermarking is an effective technique used to embed additional information into the media to be protected, such as a company's logo or a customer's hash number. Such information can later be extracted and used to authenticate ownership, detect forgery and unauthorized usage. The media being protected is called a host or cover media; and, the embedded information is called a watermark.

Watermark embedding can be implemented either in spatial domain or transform domain [1]. In spatial domain technique, the watermark embedding is done by directly modifying the pixel values of the host image [2][3]. In transform domain technique, the host image is first converted into frequency domain by a transformation method such as the discrete cosine transform (DCT) or discrete wavelet transform (DWT) [4][5]. Then, watermark is embedded by modifying its coefficients. Modifications are done by changing one or more of the bit planes of the pixel values or the coefficients in such a way that they do not perceptibly change the host image. Recently, many watermarking schemes have been proposed in the literature for digital images.

A digital image watermarking scheme must at least satisfy the requirements of robustness, imperceptibility and reasonable capacity. A watermarking system is considered robust if the embedded watermark remains detectable or retrievable under various attacks on the watermarked host, such as cropping, filtering, noise addition, geometric distortions and others. Invisible watermarking ensures unhindered viewing of the image content. Imperceptibility is

the measure of the quality of the watermarked image compared to its original host image. To have good imperceptibility, a watermarked image must appear the same to its original host image. Capacity is the size of the embedded information. Increasing capacity usually degrades the imperceptibility property.

A common attack employed on watermarked image is Salt and Pepper attack. Digital images corrupted by Salt and Pepper noise often occur in practice, due to faulty memory locations in hardware, channel decoder damages, dying down of signal in communication links, multi path wireless communication links, multi path wireless communications and transmission in noisy channel [6]. In [6-12], the watermarking systems are not robust against Salt and Pepper attack. Relatively severe Salt and Pepper attack performed on such watermarked image destroys the capability of the schemes to detect the watermark.

In this paper, a new watermarking scheme that is robust against Salt and Pepper attack using Sudoku is proposed. It is based on Sudoku's permutation property that allows evenly distributed and tightly related copies of watermark pieces in all parts of the cover image. A Sudoku solution is used during the embedding as well as during the detection of the watermark. Using classic 9x9 Sudoku, the scheme demonstrated robustness against Salt and Pepper attack close to 80% noise density.

The rest of this paper is organized as follows. In section 2, related work will be discussed. The details of our approach are discussed in section 3. The result and discussion of experiments will be covered in section 4. Finally, section 5 is for the conclusion.

2 RELATED WORK

2.1 Salt and Pepper

Once a hiding place has been decided (i.e. either in spatial or transform domain), a hiding scheme must be designed to be robust enough against various watermarking attacks. We are particularly interested in investigating and designing a scheme that is robust against salt and pepper attack. Salt and Pepper noise alter the pixel value to either minimal(0) or maximal(255) for 8 bit gray scale image [6]. Consequently, salt and pepper discretely modifies the original content of the picture in both spatial and frequency domain. As reported in Song et al, the effect of Salt and Pepper is similar to a Gaussian noise attack in which it increases the variation in pixel values in spatial domain and it has similar effect to a high pass filter in frequency domain [13]. Higher density attack will eventually modify almost all pixel values to 0 or 255 thereby destroying the watermark. Figure 1 shows an example of a noise attack at different level of noise density.

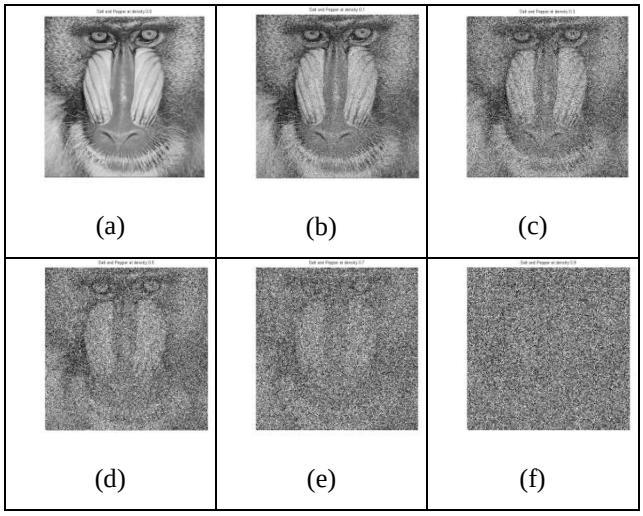


Figure 1. An image attacked with Salt and Pepper at density (a)0.0, (b)0.1, (c)0.3, (d)0.5, (e)0.7 and (f)0.9

We review here how current approaches fare against salt and pepper attacks. This is summarized in Table 1. Table 1 shows that most recent approaches could only handle Salt and Pepper noise density in the maximum range of 0.7 of the watermarked image. Rohith et al. used repetition codes for a single watermark spread over the host image [6]. Due to its error correcting code algorithm, the the recovery of the watermark has improved but significantly drop after 40% noise density. Similarly, Kaushik Pal et al's used 8 redundant copies of hidden information in HL and LH bands in Wavelet domain to recover reasonably good watermark at around 40% noise density [7].

Table 1. Comparison of Approaches against Salt and Pepper Attack

Scheme	**Method Used**	**Number of Watermark**	**Maximum Noise Density Supported (*)**	**Blind Scheme**
Rohith et. al (2012) [6]	Repetition codes	1	0.4	Blind
Kaushik Pal et. al (2012) [7]	Bit Replacement and Majority Algo	8	0.4	Non-Blind
Mehdi Khalili (2011) [8]	CDMA on DWT and Arnold Transform	1	0.5	Blind
Nallagarla Ramamurthy (2012) [9]	Quantization and Back Propagation	1	0.2	Blind
Feng and Chen (2012) [10]	Super Resolution Image Reconstruction with Repetition Encoder	1	0.1-0.2	Non-Blind
Ning Bi et al (2007) [11]	Emperical Mode Decomposition	1	0.3	Blind
Ibrahim Nasir et al (2010) [12]	Block Probability	4	0.7	Non-blind

(*) as reported in their corresponding paper. NCC (Normalized Cross Correlation) must be greater than 0.6 and BER (Bit Error Rate) must be less than 0.2.

Mehdi Khalili proposed a CDMA watermarking algorithm using 2-level DWT and Arnold Transform were able to sustain 50% noise density but performance differs between images with different contents [8]. While Nallagarla and Varadarajan used 3 level DWT with a fuzzy logic approach sustained 20% noise density but obtain watermark with quite low PSNR (+/- 20) [9]. Feng and Chen developed a watermarking technique based on super resolution image reconstruction with (3,12) convolution encoder and (3,1) repetition encoder embedded in the low frequency of a DWT image that can sustain only 10-20% salt and pepper noise density [10]. Using multiband wavelet transformation and empirical mode decomposition, Ning Bi et al achieve up to 30% noise density [11]. Ibrahim Nasir et al embed 4 redundant watermarks at 4 fixed locations using a block probability in spatial domain and able to sustain noise density at 70% but it is non-blind scheme [12]. In both spatial domain and frequencies domain, none of the above technique exceeded 70% noise density except in [12] but it is a non-blind scheme which requires the original host image. Therefore, generally, most of them cannot support Salt and Pepper attacks with noise density more than 70%.

2.2 Sudoku

A Sudoku puzzle consists of a partially completed row-column grid of cells partitioned into N regions each of size N cells, to be filled in using a set of N distinct symbols (for example, the numbers {1, ..., N}). A digit must be assigned to each cell in the grid with only one restriction: a given digit cannot appear twice in a row, in a column or in a block (region) [14]. A classic Sudoku is a puzzle whose objective is using the digits from 1 to 9 to fill a 9 × 9 grid. A solution of this type of Sudoku grid satisfies the following properties. First, a Sudoku grid contains nine 3 × 3 regions, each containing different digits from 1 to 9. Second, each row and each column of a Sudoku grid also contain different digits from 1 to 9. Figure 2 shows an example of a Sudoku solution.

One of the most important properties of Sudoku is that its constraints enforce evenly spread symbols/numbers across the board. In virtually all

sections of the board, almost all tiles' numbers can be gathered to form a complete set of tiles. Another important property of Sudoku is its number of unique solutions. Having a unique solution guarantees correct and unique sequence must be achieved horizontally, vertically and diagonally around a particular tile. In 2005, Felgenhauer and Jarvis [15] analyze the classic 9 × 9 Sudoku solutions to show that total number of possible solutions is ≈ 6.671 × 1021. The result was derived through logic and brute force computation. In 2007, Russell and Jarvis [16] showed that if various possible symmetries (e.g. rotation, reflection, and so on.) are allowed, then the number of fundamental solutions of 9 × 9 Sudoku grid is 5,472,730,538. The number of valid Sudoku solution grids for the 16×16 derivation is unknown.

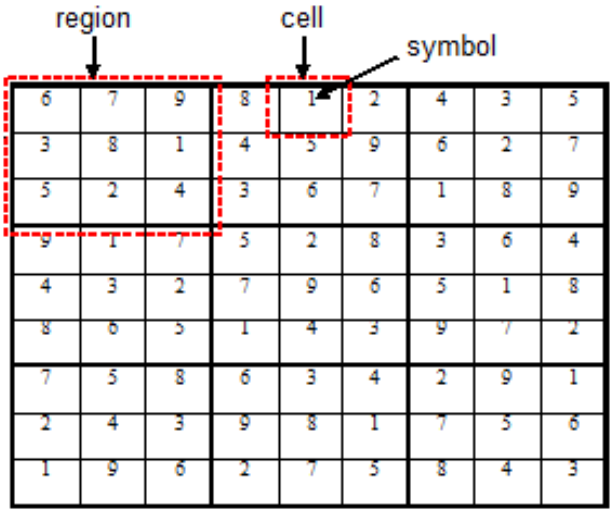


Figure 2. An example of a Sudoku solution

2.3 Sudoku Approach in Security and Data Hiding

Sudoku pattern has been employed in relatively few works in security and data hiding applications [17]. Wu and Ren [18] proposed an image authentication system using Sudoku and chaotic map. A selected Sudoku solution is used to guide cover pixels' modification in order to imply secret data. In another experiment, using Sudoku pairs, blocks scrambling and bits scrambling are applied to a cover image to completely scatter image contents [19]. Chou, Lin, Li and Li [20] proposed a data hiding scheme using Sudoku to spread out original image into three shadows images carrying the secret data. Retrieving requires a pairing of at least two shadow images. This is also done in Chang, Lin, Wang and Li [21] with lossless recovery of the embedded secret. Yet another extension to the "shadow-Sudoku" technique is done by Roshan, Rohith, Mukund, Rohan and Shanta [22] by extending the work to use pairs from color images (eg. red and green components) and, use 27x27 reference matrix instead of 256x256. Naini et al. [17] proposed a watermarking scheme using Sudoku that is robust against JPEG compression. Bits of the secret message are embedded along an edge using 16x16 Sudoku's non-repeating numbers. The authors said the scheme is also robust against cropping but mentioned "the robustness against cropping attack depends on the cropped region."

3 SUDOKU-BASED REDUNDANT WATERMARKING (SURE) APPROACH

A stronger watermarking technique is to have more than one copies of the watermark at various locations in the host image. Image watermarking systems commonly use redundant embedding to handle cropping, filtering and addition of band-limited noise [23]. Despite attempts to remove the watermark, having redundancies like this will facilitate successful detection or retrieval of the watermark. The proposed watermarking system makes use of the excellent redundancy property of Sudoku to enhance recovery of a watermark due to Salt and Pepper attack.

3.1 Embedding Procedure

Consider a cover image, C has $h_c \times w_c$ pixels and a watermark image, W_{orig} has $h_w \times w_w$ pixels. A Sudoku solution, S consists of row-column grid of cells, partitioned into N regions each of size $N * N$ cells, to be filled in using a set of N distinct symbols. A Sudoku cell, $S_{i,j}$ denotes a cell where i is the position of the cell in a region and j is the position of the region in S. For example, a third

cell in the forth region of S will be denoted as $S_{3,4}$. A value, v can be assigned to a cell where v ranges from 1..$N * N$, which is constrained by the Sudoku requirements, $\boldsymbol{R}$ – each rows, columns and regions must contain all the numbers and no repeat. It can be represented as:

$$S_{i,j} = v_{i,j} \; where \; v \in 1..N * N \; and \; \boldsymbol{R} \; is \; true \tag{1}$$

The region size, RS of a Sudoku S can be calculated as:

$$RS_{row} = \left\lfloor \left\lfloor \frac{h_c}{h_w} \right\rfloor / h_w \right\rfloor * 3 \tag{2}$$

$$RS_{column} = \left\lfloor \left\lfloor \frac{w_c}{w_w} \right\rfloor / w_w \right\rfloor * 3 \tag{3}$$

To get a watermark that can fit a region, W_{fr} the original watermark, W_{orig} need to be shrunk to a region size RS, which can be represented by:

$$W_{fr} = resize(W_{orig}, RS) \tag{4}$$

As each region must have NxN symbols, W_{fr} will be divided into NxN tiles to form W_t represented by:

$$W_t = \left\{ W_{fr_1}, W_{fr_2}, \ldots W_{fr_{N*N}} \right\} \tag{5}$$

Using W_t tiles and the Sudoku solution S, a full board watermark image, W_{FBW} can be constructed, represented by the following formula:

$$W_{FBW} = \sum_{j=1}^{N*N} \sum_{i=1}^{N*N} W_{T_k} where \begin{Bmatrix} k = 1 \; if \; S_{i,j} = 1 \\ k = 2 \; if \; S_{i,j} = 2 \\ k = 3 \; if \; S_{i,j} = 3 \\ k = 4 \; if \; S_{i,j} = 4 \\ k = 5 \; if \; S_{i,j} = 5 \\ \ldots \\ \ldots \\ k = N * N \; if \; S_{i,j} = N * N \end{Bmatrix} \tag{6}$$

Figure 3 shows the embedding process. It starts with two processes: 1) regions mapping of the cover image to the Sudoku regions (9 regions in total); 2) symbols generation of the watermark image by breaking it into 3x3 = 9 distinct symbols or tiles (in this paper, we use 'symbols' and 'tiles' interchangeably). The tiles are numbered from left to right, top to bottom. Based on a Sudoku solution, the watermark symbols will be re-arranged and embedded into each region of the cover image.

The end result will be 9 copies of binary watermarks being distributed in 81 tiles which is not overlapping and evenly spread in the cover image (see Figure 4 right). Changing a Sudoku solution will accordingly change the watermark tiles arrangement, but preserves its distribution property. Figure 4 illustrates the watermarked image (left) and the watermark tiles embedded inside the cover image (right).

3.2 Detection Procedure

Prior to finding the watermark in a watermarked image, the watermark tiles, W_t need to be calculated from W_{orig}. Once the raw embedded watermark is retrieved from the cropped image or a clean watermarked image, symbols searching can be done. Using symbols from W_t, a search of the tiles begins by recording the sequence of the detected tiles, Seq, represented by:

$$Seq = sym\_search(W_t, W_{ret}) \tag{7}$$

The sequence information in Seq is matched with the one in the Sudoku solution, S. From the matches, the detection result, D will indicate a successful or a failed detection.

$$D = \begin{Bmatrix} yes \; if \; Seq \cap S \neq \emptyset \\ no \; if \; Seq \cap S = \emptyset \end{Bmatrix} \tag{8}$$

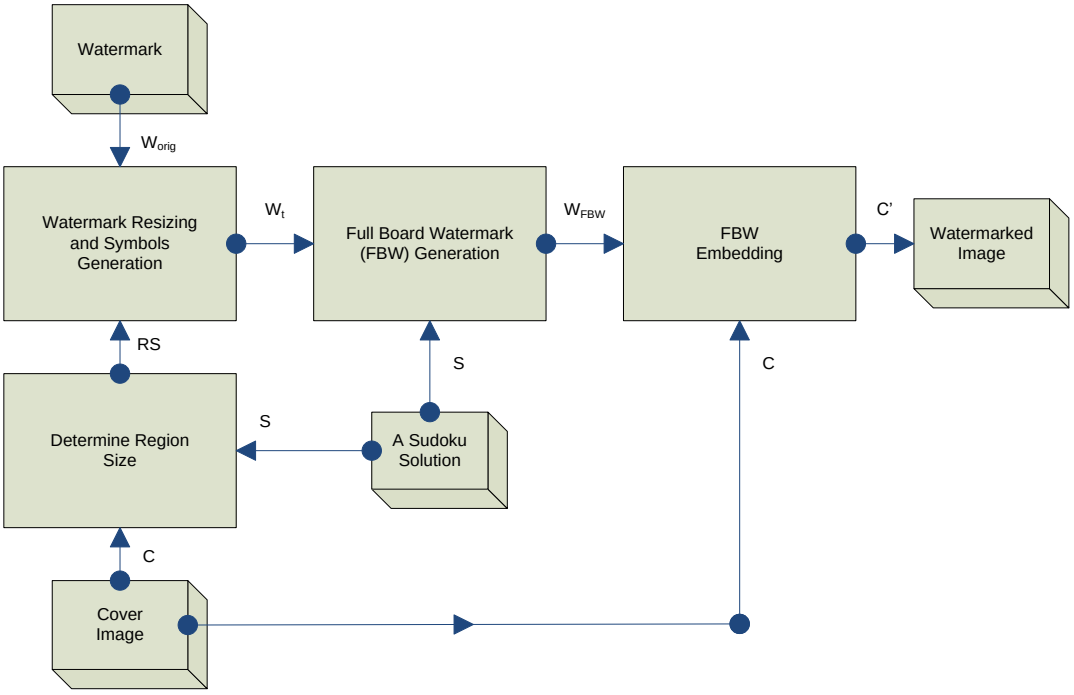


Figure 3. The embedding process of SURE

Figure 4. A watermarked pepper cover image with baboon inside it(left). The 81 baboon watermark tiles (right)

Figure 5 shows the process of watermark detection. Using the same watermark used in the embedding process, nine symbols will be generated. Then, a raw watermark will be retrieved from the original watermarked image. It follows with searching each of the watermark symbols in the retrieved raw watermark. The outcome will consist of complete and partial tiles as shown in Figure 6. During the search, the sequence of the complete tile(s) is recorded. Then, the sequence analysis engine will check if the sequence matches with the one in the supplied Sudoku solution – horizontally and vertically around the detected tile(s).

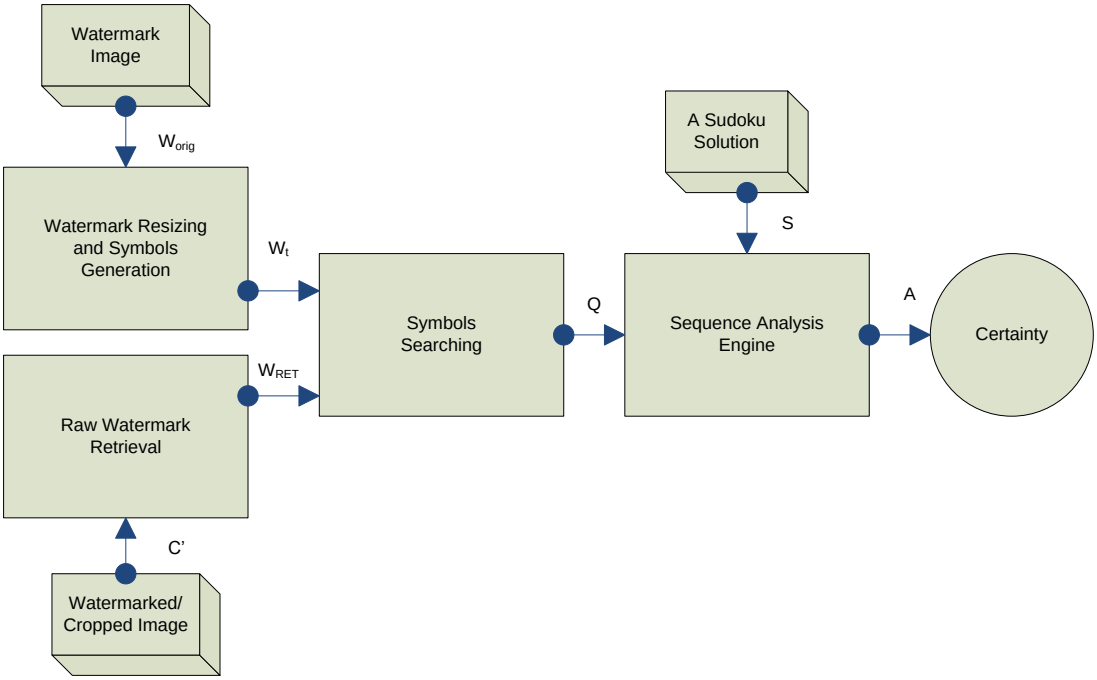


Figure 5. The watermark detection process of SURE

Figure 6. A cropped image and the watermark tiles embedded in it.

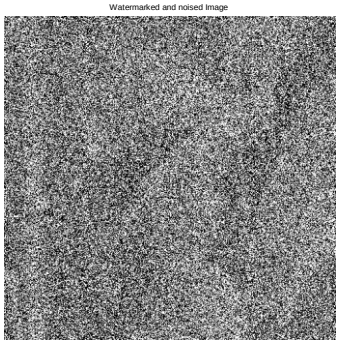
4 RESULTS AND DISCUSSION

The proposed watermarking system was implemented on a standard notebook and tested with standard images commonly used in watermarking research. Each watermarked image is attacked with 1000 random Salt and Pepper attacks at 3 different level of noises (75%, 80% and 90%). 8 set of cover images were used with 8 set of watermarks. Therefore, the total random tests are 24000.

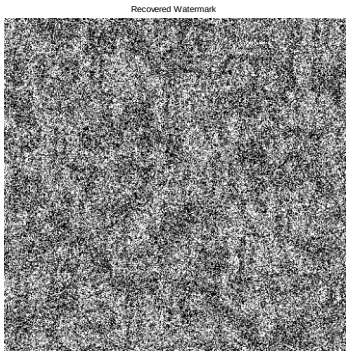
Before the Salt and Pepper noise is applied, the average PSNR for all watermarked images are well above normal watermarking schemes (35-40dB). Figure 7 demonstrates a watermarked image of Lena that has been attacked with a random noise of 80%. As expected, the retrieved watermark accumulates noises like its host. However, using sequence information between neigbouring tiles and other regions, the watermark can still be detected. We demonstrate how this work with the following example.

(a)

(b)



(c)



(d)

Figure 7: a) the watermarked image Lena; b) the watermark image baboon; c) the watermarked image with extreme noise applied to it; d) the retrieved waterwark

In the Figure 7, the following Sudoku has been used:

[7,2,6,3,1,5,4,8,9][4,9,3,7,2,8,6,5,1][8,1,5,9,4,6,2,3,7]
[8,5,2,6,7,3,9,4,1][1,4,7,9,8,5,3,6,2][6,9,3,1,2,4,7,5,8]
[1,9,4,5,6,7,2,3,8][8,3,6,2,1,4,5,7,9][5,7,2,3,8,9,4,6,1]

From the retrieved watermark, the following tiles have been recovered (Figure 8). The one with 0 indicates the tile is not recognizable. Notice the recovered tiles matches the correct sequence of the Sudoku above. They are at the right location and in the right sequence. At 80% noise, 44 out of 81 tiles have been recovered. On average at least 4 redundant tiles is available for each unique tiles.

[7,0,6,0,0,0,4,0,0][0,0,3,0,2,8,0,5,0][0,1,5,9,4,0,2,3,7]
[0,5,2,0,0,3,0,0,0][1,0,7,9,8,5,3,6,0][6,9,0,0,2,4,0,0,8]
[1,0,4,5,0,0,0,3,8][0,3,6,2,0,0,5,7,0][0,7,0,0,8,9,4,0,1]

Figure 8: Recovered tiles

Table 2 demonstrates a stripe of the experimental results set with noise level at 80%. The first row (Test ID #371) indicates the number of tiles recovered for each unique tiles – we detected 6 tile #1, 3 tiles #2, and so on. On the eight row (Test ID #378), we manage to recover only 2 tiles #2. In our scheme, to identify weather the image have been watermarked or not specifically by our scheme, we do not really need to recover all of the tiles. The location of a specific tile (eg. tile #5) must be retrieved from the exact location. For example, we manage to recover tile #7 from 8 different regions, and these tiles must be at correct location in each regions. These multiple redundancies enhance the certainty if it has been watermarked by our scheme.

Table 2. Experiment 2B: with Salt-n-Peppper level 0.80, Baboon inside Lena

	Tile Number								
TestID	T1	T2	T3	T4	T5	T6	T7	T8	T9
371	6	3	5	6	5	5	7	7	5
372	3	5	6	5	3	5	3	4	3
373	5	4	6	5	4	4	4	2	4
374	3	2	6	5	3	4	8	4	4
375	2	4	8	4	6	7	4	5	6
376	3	6	4	3	7	4	5	3	7
377	5	6	3	3	6	7	5	6	4
378	6	2	4	4	4	6	4	6	7
379	3	2	4	2	4	3	7	4	5

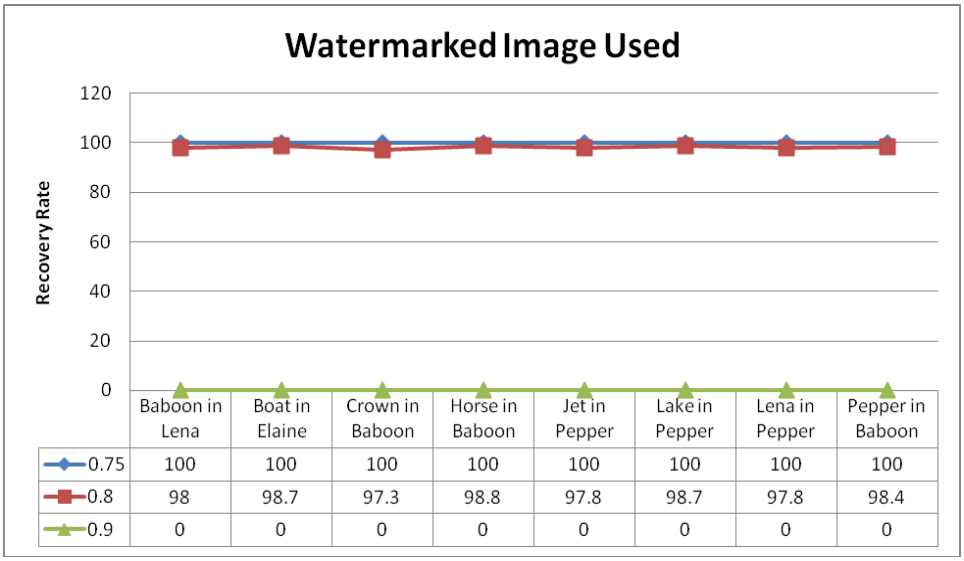


Figure 9. The effect of different image content on the recovery rates

In these experiments, we randomly mix standard images within one another to normalize the effect of image content versus the recovery rate achieved. With different content of hosts and watermarks, the scheme demonstrates consistencies in its recovery rate (see Figure 9). In current experiments, it shows that with 0.8 noise density, the probability of full recovery is at least 97%. It is important to note that standard images used in the experiments (whether chosen as a host or watermark) *do* represent normal images taken in daily photos. Variations between neighboring pixels are commonly seen in normal photos. Table 3 shows the comparison of our approach with other watermarking schemes. The detection capability of Soduku-based watermarking under severe Salt-n-Pepper attack significantly exceeded the rest. An important feature of the proposed technique is its ability to detect watermark from incomplete tiles recovery.

Table 3. Comparison of Sudoku based redundant watermarking with other watermarking schemes

	Maximum Density of Salt and Pepper Attack Sustained	Number of watermark	Blind Retrieval
Other schemes	10-70%	1-8 copies	Mixed
Sudoku based Redundant Watermarking (SURE)	78%	9 copies	Blind. (*)

(*) Original cover image is not needed to extract the watermark. The SURE watermark detector can be distributed with a fixed and encrypted or hardcoded watermark. As there is no relationship between the watermark and the cover image (i.e. one cannot derive the other), SURE can be considered a blind watermarking scheme. Refer to blind watermarking discussion in [23].

The Sudoku's unique symbol permutation and its evenly distributed tiles effectively leave sufficient "pattern of traces" to support detection, even under severe random noises. Furthermore, it also offers greater practicality as a blind watermarking scheme.

5 CONCLUSION

In this paper, a novel watermarking scheme based on Sudoku's permutation property is proposed, which embed watermark pieces into a host image in a precise and organized pattern. This pattern information significantly improves detection of the watermarks. The proposed watermarking scheme was tested with natural photo images taken from standard image libraries. Watermarked images were attacked with the Salt n Pepper noise as high as possible. The 81 tiles 9x9 Sudoku configuration were completely able to resist up to 78% noise density before it went down to 97% recovery at 80% noise density. A 256 tiles-16x16 configuration may further improve the detection performance due to the availability of greater number of tiles and watermark traces. Furthermore, with such configuration, the number of Sudoku permutation will increase exponentially, and therefore making it more secure from watermark removal. Other experiments are on the way to spread the Sudoku redundancies across multiple domain.

6 ACKNOWLEDGEMENTS

This work is supported by Universiti Tun Hussein Onn Malaysia. The grant number is UTHM-FRGS-1051.

7 REFERENCES

[1] C. W. H. Fung, A. Gortan and W. Godoy Jr., A Review Study on Image Digital Watermarking, in: Proceedings of the 10th International Conference on Networks ICN2011, 2011, pp. 24-28.

[2] Y. G. Fu, R. M. Shen, Color Image Watermarking Scheme Based on Linear Discriminant Analysis, Computer Standards and Interfaces vol. 30(3), 2008, pp. 115-120.

[3] A. Aggarwal, M. Singla, Robust Watermarking of Color Image under Noise and Cropping Attack in Spatial Domain, International Journal of Computer Science and Information Technologies, vol. 2(5), 2011, pp. 2036-2041.

[4] V. P. Reddy, S. Varadarajan, An Effective Wavelet-based Watermarking Scheme using Human Visual System for Protecting Copyrights of Digital Images, International Journal of Computer and Electrical Engineering, vol. 2(1), 2010, pp. 24-27.

[5] D. Kundur, D. Hatzinakos, Towards Robust Logo Watermarking using Multi-resolution Image Fusion, IEEE Transactions on Multimedia, vol. 6(1), 2004, pp. 185-197.

[6] S. Rohith, K.N.H. Bhat, A simple Robust Digital Image Watermarking against Salt and Pepper Noise using Repetition Codes, International Journal on Signal and Image Processing, vol. 3(1), 2012, pp. 47-54.

[7] K. Pal, G. Ghosh, M. Bhatarcharya, Biomedical Image Watermarking in Wavelet Domain for Data Integrity Using Bit Majority Algorithm and Multiple Copies of Hidden Information, American Journal Of Biomedical Engineering, vol. 2(2), 2012, pp. 29-37.

[8] M. Khalili, A Novel Effective, Secure and Robust CDMA Digital Image Watermarking in YUV Color Space Using DWT2, International Journal of Computer Science Issues, vol. 8(3), 2011, pp. 70-78.

[9] N. Ramamurthy, S. Varadarajan, The Robust Digital Image Watermarking using quantization and Fuzzy Logic Approach in DWT Domain, International Journal of Computer Science and Network, vol. 1(5), 2012, pp. 13-19.

[10] X. Feng, Y. Chen, Digital Image Watermarking Based on Super Resolution Image Reconstruction, Proceeding of the International Conference on Fuzzy Systems and Knowledge Discovery, 2012, pp. 1778-1782.

[11] N. Bi, Q. Sun, D. Huang, Z. Yang, J. Huang, Robust Image Watermarking based on Multiband Wavelets and

[12] Empirical Mode Decomposition, IEEE Transactions on Image Processing, vol. 16(8), 2007, pp. 1956-1966.

[13] I. Nasir, F. Khelifi, J. M. Jiang, S. S. Ipson, A Robust Image Watermarking Scheme based on Normalized Circular Image in DWT Domain. Proceedings of the 10th International Conference on Information Sciences, Signal Processing and their Applications (ISSPA2010), 2010, pp. 33-36

[14] C. Song, S. Sudirman, M. Merabti, A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks, Proceedings of the 11th of PostGraduate Network Symposium (PGNET), 2010, pp. 119-124.

[15] N. Jussien, A to Z of Sudoku, London: ISTE Ltd, 2007.

[16] B. Felgenhauer, F. Jarvis, Mathematics of Sudoku I, Mathematical Spectrum, vol. 39(1), 2006, pp. 15-22.

[17] E. Russell, F. Jarvis, Mathematics of Sudoku II, Mathematical Spectrum, vol. 39(2), 2007, pp. 54-58.

[18] P. M. Naini, S. M. Fakhraie, A. N. Avanaki, Sudoku Bit Arrangement for Combined Demosaicking and Watermarking in Digital Camera, in: Proceedings of the IEEE 2nd International Conference on Advances in Databases, Knowledge, and Data Applications, 2010, pp. 41-44.

[19] W. C. Wu, G. R. Ren, A New Approach to Image Authentication using Chaotic Map and Sudoku Puzzle, in: Proceedings of the IEEE Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009, pp. 628-631.

[20] Y. Zou, X. L. Tian, S. W. Xia, Y. Song, A Novel Image Scrambling Algorithm based on Sudoku Puzzle, in: Proceedings of the IEEE Forth International Congress on Image and Signal Processing, 2011, pp. 737-740.

[21] Y. C. Chou, C. H. Lin, P. C. Li, Y. C. Li, A (2,3) Threshold Secret Sharing Scheme using Sudoku, in: Proceedings of the IEEE Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010, pp. 43-46.

[22] C. C. Chang, P. Y. Lin, Z. H. Wang, M. C, Li, A Sudoku-based Secret Image Sharing Scheme with Reversibility, Journal of Communications, Academy Publisher, vol. 5(1), 2010, pp. 5-12.

[23] B. R. Roshan Shetty, J. Rohith, V. Mukund, H. Rohan, Steganography using Sudoku Puzzle, in: Proceedings of the IEEE International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 623-626.

[24] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Morgan Kaufmann: Burlington, MA, 2008.