IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

An Improved Mapping Pattern for Digital Watermarking using Hilbert-Peano Pattern

To cite this article: Mohamad Nazmi Nasir *et al* 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **769** 012009

IOP Conf. Series: Materials Science and Engineering **769** (2020) 012009 doi:10.1088/1757-899X/769/1/012009

An Improved Mapping Pattern for Digital Watermarking using Hilbert-Peano Pattern

Mohamad Nazmi Nasir, Syifak Izhar Hisham, Mohd Faizal Ab Razak

Faculty of Computing, Universiti Malaysia Pahang, 26300 Gambang, Pahang, Malaysia

syifakizhar@ump.edu.my

Abstract. In the present, watermark plays an important part in all copyrighted content whether it is physical or digital. The importance of watermark in digital data increases as the usage of internet in transferring data increases day by day as the technologies improves. The main objective of using digital watermark is to apply the highest security as possible to the digital image and in the same time to reduce as most disturbance as possible that can be visible to the human eye. This research proposed a hybrid mapping pattern which is Hilbert-Peano Curve to try to achieve the highest security as possible from alteration. This proposed digital watermark uses the Least Significant Bit (LSB) to store the watermark data, which consist of parity bits as the authentication data and recovery data. This is to reduce the disturbance to the original image as much as possible as it might alter the colour of the original image. The results are compared with the existing watermark, Hilbert-LSB to analyse which pattern is suitable to be implemented with the watermarking scheme. The results of this research shows Hilbert-Peano pattern can contribute better performance in terms of watermark data security, time taken to embed watermark data, and the imperceptibility level if compared to the original Hilbert mapping pattern.

1. Introduction

In the process of sharing information on the internet, security play a big role in ensuring the data transferred from the sender arrives to the receiver without any disturbance from an unknown entity that might be stealing any information from the transferred data. All of the data on the internet should be kept secret from the others except the sender and servers since that the data may be security-sensitive [1]. The data also requires authentication to provide confirmation on the authenticity of the data. The data also must be confirmed that it does not been tampered by any outside entity.

The most known data security techniques can be classified into two categories: Digital watermarking and steganography. Digital watermarking is a capability for inserting information known as watermark, into an image which later can be extracted or observed for various purposes such as identification and authentication [2-7]. Besides providing security, this technique can also be utilized to gain information about the source, owner, distributor or creator of an image or a document. The second category is steganography which focuses more on bandwidth of the hidden messages while hiding a message, file or an image within another message, file or image but in the aspect of watermarking, the watermark robustness is the key performance parameter [8-9].

Two fragile watermarking schemes SPIRAL-LSB and HILBERT-LSB for authentication have been developed with the special feature of embedding [10-13]. They applied unique pattern of numbering to decide the watermark bit locations. These schemes have extended the current technology of fragile watermarking. The watermarked images age proven theoretically and experimentally as good and qualified to use in clinical diagnosis. The accepted noise for human sight is 32dB, and they managed to get below this value. However, the current watermarking pattern took some time to embed the watermark into the images. Thus, the research is to test whether the proposed watermarking pattern is faster than the current watermarking pattern available.

2. Hilbert-Peano Authentication Scheme

2.1. Generating the Hilbert-Peano Pattern

2.1.1. Divide the Hilbert-Peano Pattern. Based on the Hilbert-Peano pattern, the pattern is generated by using two basic elements, corresponding to the connected curve. Figure 1 shows the two basic elements of the pattern.

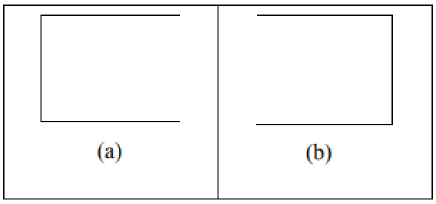


Figure 1. Basic generated elements

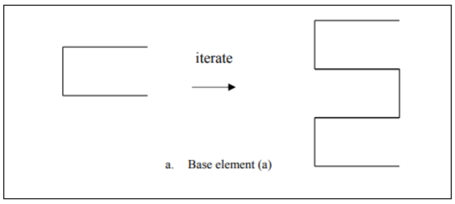


Figure 2. Generation of the pattern

2.1.2. Iterative Matrix. The Hilbert-Peano pattern generating element is simple but according to its characteristics, as the number of iterations increases, the number of the iteration of the infinity curve will traverse the area within the scope of all of the points. Based on the curve of each iteration characteristics, the amplification of iterative matrix is applied to describe the curve generation process, as demonstrated in Figure 2. The generation of the curve for the first iteration will be as in Figure 2.

2.1.3. The Connection Between the Generated Curve. According to the characteristics of the Hilbert-Peano pattern, the curve has one entrance and one exit meaning that the repeated traversal area must demand the curve to be continuous at all squares. By the n number of iterations of the Hilbert-Peano pattern after it has been translated to a $6n \times 6n$ iterative matrix according to the rules.

2.2. Numbering and Embedding the Watermark Bits

The detailed embedding algorithm of this authentication watermarking are described in [10-13]. Before the embedding process, all the blocks in the image are numbered and mapped with the mapping pattern to determine the location and mark the blocks as the watermarked data to avoid redundancy in the embedding process. By using a specific style of numbering and mapping of each block, it could assure the top performance of the authentication system by spreading the numbered data as far as possible from the original location. The numbering of the block is determined on the user whether they want to divide the block into 6 by 6 smaller blocks or 8x8 even smaller blocks.

The blocks of the original images are labelled as C and the blocks of watermarked image as H. The proposed mapping pattern starts with numbering C using the Hilbert-Peano method and map it using the pseudorandom way. The numbering then will start at a random pixel and then followed by moving to the next block. All of the block then will be embedded and numbered.

In the process of generating the Hilbert-Peano pattern, it follows a recursive algorithm as follows:
Step 1: Set the block size as C,
Step 2: Set k as the key number,
Step 3: Calculate the number of blocks to get the total number of columns and rows,
Step 4: Choose the starting point then start the block numbering,

IOP Conf. Series: Materials Science and Engineering **769** (2020) 012009 doi:10.1088/1757-899X/769/1/012009

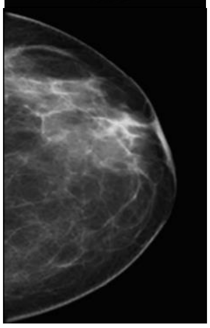
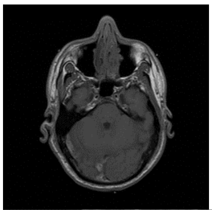
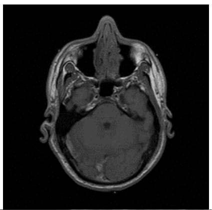
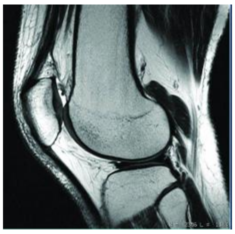
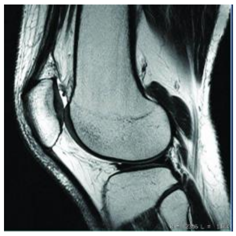
Step 5: After the block numbering is completed, each block then will be mapped using the mapping pattern presented in [10-13].

3. Experimental Results and Discussion

3.1. Imperceptibility by Visual

The embedded watermark in medical images are not clearly visible to the naked eye at it is embedded in the Least Significant Bit (LSB). From Table 1, it is obvious to say there is no difference between the original and watermarked images. Therefore, to measure the imperceptibility of the watermarked images accurately, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) is preferred for measurement.

Table 1: Comparison between the Original and Watermarked Images

Original Image	Watermarked Image	Original Image	Watermarked Image
			
			
			
			

3.2. Peak Signal to Noise Ratio (PSNR)

PSNR is the ratio between a power of the signal noise and the signal's maximum power.

It is used to measure the quality of the images that has been embedded watermark into it. If the PSNR value is high, it means that the image is almost similar with the original image. Hence, each image will be embedded into two watermarking pattern and the value of the PSNR will be compared.

Table 2 shows the PSNR values obtained from the two watermarking pattern that is used in this research, Hilbert-LSB (11, 14) and Hilbert-Peano.

Table 2: PSNR Values between Hilbert-LSB and Hilbert-Peano watermarking pattern

Figure	PSNR of Hilbert-LSB	PSNR of Hilbert-Peano
Sample 1	58.9348	58.9406
Sample 2	58.8268	58.8912
Sample 3	53.9764	53.6794
Sample 4	58.3968	58.3872
Sample 5	55.4978	55.5138
Sample 6	58.4014	58.4297
Sample 7	58.6310	58.6431
Sample 8	58.6851	58.6851
Average Value	**57.6463**	**57.6687**

Table 2 shows the result of PSNR values gained from both the image watermarking schemes on the medical images that is tested on 8 different samples. The amount of PSNR value is calculated based on the ration between the power of distorting noise that affects the quality of the watermarked image and the maximum possible value of a signal.

Based on the average value of PSNR, the Hilbert watermarking scheme is lower by 2 decimal places if compared to the proposed scheme. As we know, the lower the PSNR value, the better the security of the image but based on these results, there was not much difference in PSNR value in comparison between both of the values.

3.3. Mean Square Error (MSE)

Mean Square Error (MSE) defines as the cumulative squared error between the original image and the embedded image. The lower the MSE value, the lesser the error found in the watermarked image meaning that the alteration on the embedded image is less significant to the naked eye. The same sample images will be tested on the MSE and the outcome is recorded.

Table 3 shows the MSE values obtained from the two watermarking pattern that is used in this research.

Table 3: MSE Values between Hilbert-LSB and Hilbert-Peano watermarking pattern

Figure	MSE Value of Hilbert-LSB	MSE Value of Hilbert-Peano Scheme
Sample 1	0.0830	0.0831
Sample 2	0.0839	0.0852
Sample 3	0.2787	0.2787
Sample 4	0.0943	0.0941
Sample 5	0.1827	0.1834
Sample 6	0.0933	0.0940
Sample 7	0.0889	0.0891
Sample 8	0.0880	0.0880
Average Value	**0.1241**	**0.1244**

3.4. Embedding Processing Time

The embedding process is the process of inserting the watermark into the original image. Hilbert Pattern is a single type pattern and Hilbert-Peano is a hybrid pattern as it combines two patterns into one.

Table 4 shows the time taken to embed the watermark into the images. The images are varying in sizes as they are different medical images. The size of the images also affected the time taken for the watermark to embed into the images.

Table 4: Time taken comparison between Hilbert-LSB and Hilbert-Peano watermarking pattern.

Image Sample	Image Size	Hilbert-LSB	Hilbert-Peano
		Time Taken	Time Taken
Sample 1	537 KB	45.9219	37.7813
Sample 2	645 KB	55.8750	44.8906
Sample 3	65.0 KB	5.6563	4.4844
Sample 4	1.43 MB	510.7969	408.6719
Sample 5	301 MB	351.9219	338.8594
Sample 6	101 MB	303.0781	275.1406
Sample 7	960 KB	375.8125	336.0625
Sample 8	5.39 KB	13.8750	13.0313
Average Value		**207.8672**	**182.36525**

In the table, the time taken differs and the bigger the size of the image, the longer time is needed to embed the watermark. From the table, it is clear that the Hilbert pattern is taking a bit longer time to embed as compared to the Hilbert-Peano pattern. This is because of the embedding process of the Hilbert watermarking scheme requires a 2-bit information authentication data size and 7 bits for the recovery information for each pixel as compared to the Hilbert-Peano watermarking scheme which is less.

4. Conclusion

The proposed watermarking scheme has proved better in terms of the time processing of embedding the watermark into the medical images. The quality of the PSNR and the MSE value was not significantly different meaning that the quality of the image is not too much disturbed by the watermark. This proves that even though the proposed watermark is a hybrid, it does not affect much on the watermarked image. The proposed watermarking can be used if it involves a large amount of data in order to reduce the processing time for image watermarking.

Acknowledgments:
This research work is supported by RDU1803163 supported by Universiti Malaysia Pahang. The data in this paper can be accessed in the website of FKom, UMP at [http://fskkp.ump.edu.my].

References

[1] Singh, G. (2018). A review of secure medical image watermarking. IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017, 3105–3109. https://doi.org/10.1109/ICPCSI.2017.8392297
[2] Araghi, T. K., Manaf, A. B. A., Zamani, M., & Araghi, S. K. (2016). A Survey on Digital Image Watermarking Techniques in Spatial and Transform Domains. International Journal of Advances in Image Processing Techniques– IJIPT, 3(1), 6–10.
[3] Mantoro, T., Ayu, M. A. & Priyatna, M. A. (2018). Security Scheme based Dual-Layer Fragile Watermarking for Medical Image. 2018 Third International Conference on Informatics and Computing (ICIC), Palembang, Indonesia, pp. 1-5.
[4] Rajput, V. & Ansari, I. A. (2019). Image tamper detection and self-recovery using multiple median watermarking. Multimedia Tools and Applications, pp 1–17.
[5] Ma, B., Li, B., Wang, X., Wang, C., Li, J., & Shi, Y. (2019). A code division multiplexing and block classification-based real-time reversible data-hiding algorithm for medical images.

Journal of Real-Time Image Processing, August 2019, Volume 16, Issue 4, pp 857–869.

[6] Liu, X., Lou, J., Fang, H., Chen, Y., Ouyang, P., Wang, Y., Zou, B., & Wang, L. (2019). A Novel Robust Reversible Watermarking Scheme for Protecting Authenticity and Integrity of Medical Images," in IEEE Access, vol. 7, pp. 76580-76598.

[7] Rakhmawati, L., Wirawan, W. & Suwadi, S. (2019). A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability. EURASIP Journal on Image and Video Processing, December 2019, 2019:61

[8] Alias, N. & Ernawan, F. (2019). Multiple watermarking technique based on rdwt-svd and human visual characteristics. Journal of Theoretical and Applied Information Technology, Volume 97, Issue 14, Pages 3980-3939.

[9] Sharma, N. & Batra, U. (2017). A Review on Spatial Domain Technique Based on Image Steganography. 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, 24-27. 10.1109/IC3TSN.2017.8284444

[10] Ernawan, F. (2019). Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection. International Journal of Electrical & Computer Engineering (2088-8708) 9 (3).

[11] Hisham, S. I., Zain, J. M., Arshad, N. W., & Liew, S. C. (2015). HILBERT-LSB-C as authentication system for color medical images. 2015 4th International Conference on Software Engineering and Computer Systems, ICSECS 2015: Virtuous Software Solutions for Big Data, Langkawi, 15–20. https://doi.org/10.1109/ICSECS.2015.7333114

[12] Hisham, S. I., Muhammad, A. N., Zain, M. J. & Badshah, G. (2013). Localization watermarking for authentication of text images in Quran with spiral manner numbering. 2013 Taibah University International Conference on Advances in Information Technology for the Holy Quran and Its Sciences, Madinah, 24-29.

[13] Hisham, S. I., Muhammad, A. N., Zain, M. J., Badshah, G. & Arshad, N. W. (2013). Digital watermarking for recovering attack areas of medical images using spiral numbering. 2013 International Conference on Electronics, Computer and Computation (ICECCO), Antalya. 285-288.

[14] Hisham, S. I., Zain, M. J., Arshad, N. W., Liew, S. C., Johari, N. H. & Badshah, G. (2014). Authentication system for medical images using Hilbert numbering. 2014 International Conference on Computer, Communications, and Control Technology (I4CT), Melaka. 198-202.