A NOVEL COVERLESS INFORMATION HIDING TECHNIQUE USING PATTERN IMAGE SYNTHESIS

Weng Ken Lee[*], *SimYing Ong*[⋆], *KokSheik Wong*[†], *Kiyoshi Tanaka*[‡]

School of Computing and Information Technology, Taylor's University, Malaysia.[*]
Faculty of Computer Science and IT, University of Malaya, Malaysia.[⋆]
School of Information Technology, Monash University, Malaysia.[†]
Faculty of Engineering, Shinshu University, Japan.[‡]

ABSTRACT

In this paper, a novel coverless information hiding technique is proposed. Secret information is utilized as the input to synthesis pattern image with embedded secret. Three observed properties in general pattern images, including color, size and position are discussed in this paper to realize coverless information hiding. In the experiment result section, a simple prototype is built as a proof of concept. Finally, the performance of the prototype in terms of the visual image quality, embedding capacity and resistance to attacks are discussed.

Index Terms— Data Insertion, pattern image generation, pixel color, coverless data hiding

1. INTRODUCTION

Information hiding conceals information via two major methods, which are encryption and data insertion. Encryption translates confidential information into incomprehensible form to avoid unauthorized viewing. For data insertion, it embeds secret message into a carrier or hiding medium, i.e., cover. In this case, the produced output image quality after data insertion should be as similar as the cover, or at least without noticeably changes, to conceal the existence of covert communication.

Both methods are utilized in their own ways, serving different purposes. Encryption is often utilized in securing password, confidential storage data, file transmission, etc. Encryption provides high confidentiality, but it also comes with few drawbacks. Encryption not only consumes high computational cost due to its complexity, it also arouse suspicious of the attacker during transmission, since it transforms secret message into random format.

Hence, in some applications, particularly involving secret communication, data insertion is preferred than that of encryption because it hides the trace of communication without arousing suspicious of attackers or observers. Various type of data can be inserted via data insertion algorithm, including watermark to claim ownership, meta-data for media enrichment, fingerprint for copyright dispute, or simply secret message for communication purposes, etc.

There are few significant researches for data insertion using image as cover. Information hiding in least significant bit (LSB) is one of the famous techniques due to its simplicity in implementation [1, 2]. LSB for image pixels can be flipped from zero to one or one to zero to carry secret message. Besides, LSB technique can also be easily applied to different domain, including encrypted domain [3], audio [4] and video domains [5]. However, most of the proposed LSB information hiding technique suffered from data loss after the secret message extraction at the decoding process.

Histogram shifting by Ni et. al [6] is one of the earliest techniques in achieving reversibility in data insertion [7]. Reversibility means the embedded medium can be fully recovered (i.e., to the state of before embedding) after the secret message is extracted. Ni et. al utilizes pixels' frequency of occurrence in image to build a histogram. Then, the bin with highest frequency (i.e., with the most number of pixels) will be shifted to left or right to prepare a blank bin space. Pixels under the highest frequency bin and the blank bin space will be utilized for data insertion purposes. However, histogram shifting suffers from the image overflow and underflow problem. Hence, there are many variants of histogram shifting based data insertion techniques are proposed [8, 9, 10].

On the same year, Tian also proposed a novel technique, namely difference expansion to embed information into cover image[11]. Tian exploited the natural image redundancy to achieve data insertion. All the image pixels are grouped into pairs, then one bit of secret message is hidden in each pair by expanding the difference between two pixels. Tian's technique is simple but able to achieve high embedding capacity at that time. Later on, Thodi et. al proposed prediction-error expansion technique, as an improvement over Tian's technique to improve its image quality and the needs to maintain location map [12, 13]. After that, there are numerous researchers focus on improving the existing proposed techniques by enhancing the adaptivity [14, 15, 16] of both difference expansion and prediction error expansion techniques.

Although most of the researches are claiming that their techniques are secure (i.e., not arousing suspicious) after achieving high PSNR or SSIM, if attackers carefully examines the statistic of the image, the secret communication might be able to be detected. Statistical attack is one of the well known attack in information hiding[17]. It utilizes the natural statistic of cover (e.g., image, audio) to detect the existence of embedded data. For instance, LSB technique modified the last bit of every pixel to carry one bit of information. If the frequency of occurrence of zeros and ones are collected, image with embedded data will resembles similar number of zeros and ones. This is because the prior encryption of secret message forces the equally distribution of data variances. In fact, in natural image or image without embedded data, the number of zero and one should not be equal or similar.

Another type of attack in data insertion is comparison attack, by utilizing the original cover to compare with the embedded cover. Nowadays, it is not difficult to find the original cover on the Internet due to the powerful features offered by image search engine. Thus, if the attacker is able to find the original cover, the secret communication will be detected and the message can be extracted by simply comparing the covers.

Texture-based image synthesis information hiding techniques [18, 19] are proposed to overcome some of the aforementioned problems. Patches of texture are manipulated and inserted to form an output image with embedded information. However, patches are inserted in tile or block-basis, which might causes noticeable distortion or blockiness in these methods.

Therefore, in this paper, a novel coverless information hiding technique using pattern synthesis is proposed. In this technique, differs than the conventional techniques, there is no cover image involved. By utilizing solely input or secret message, the data embedding algorithm will synthesize a pattern image with embedded data.

2. CONVENTIONAL DATA INSERTION PROCESSES

In this section, the generalized encoding and decoding processes of conventional information hiding technique are illustrated.

Fig. 1 shows the conventional encoding process. First, a cover image is carefully chosen as carrier or medium to hide secret message. Second, information hiding algorithm will insert secret into the cover image with or without the added security provided by the encoding key. Finally, the embedded image is generated. Embedded image should resemble the cover image as close as possible to avoid detection. The embedded image is then sent to the receiver.

Fig. 2 illustrates the reversing or decoding process for conventional data insertion technique. First, receiver receives the embedded image via public communication channel (e.g., Internet, email). Then, the embedded image will be fed into the data extraction algorithm (with or without the decoding key, depending on the encoding process) for secret message extraction purposes. Finally, the secret message is extracted. If the data extraction algorithm recovers the cover image (i.e., exactly same as before embedding), then the technique achieves reversibility. Reversibility is a crucial property for some of the applications such as military maps, medical images, because the details of the images need to be retained after extraction.

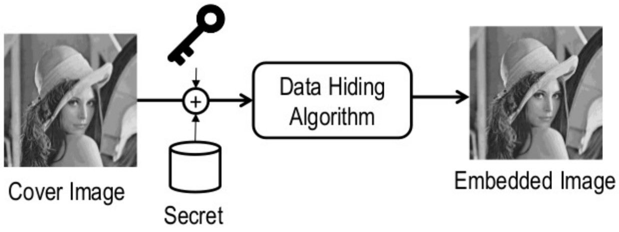


Fig. 1. Conventional Encoding Process

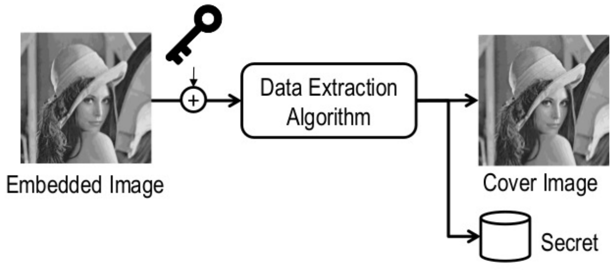


Fig. 2. Conventional Decoding Process

3. PROPOSED INFORMATION HIDING

Fig. 3 shows the encoding process of the proposed information hiding technique. As shown in the figure, there is no cover image involved in the encoding process. In the proposed encoding process, the only input needed is the secret message and encoding key. Next, pattern image with embedded message will be generated by the information hiding algorithm based on the secret message. There are few properties which can be manipulated in synthesizing pattern

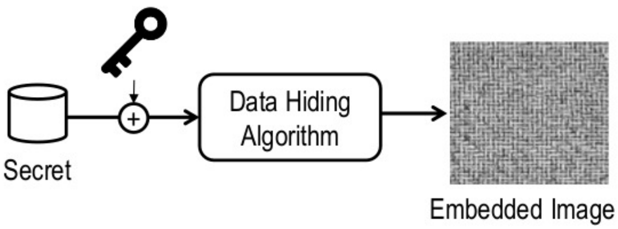
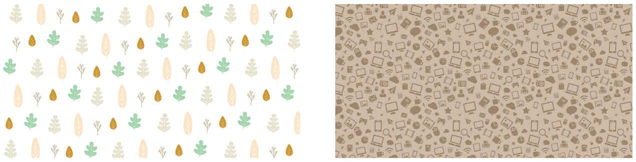


Fig. 3. Proposed Encoding Process

images (i.e., in information hiding algorithm), including positions, sizes and colors of patterns.

3.1. Position

Pattern images are sometimes formed by a number of repeatable elements, and these type of pattern images can be utilized as design to make house wallpaper, present wrapping paper, desktop or mobile devices wallpaper, etc. **Fig. 4(a)** and **Fig. 4(b)** are the examples of pattern images downloaded from the Internet. The position of the repeatable elements in these pattern images can be manipulated in the proposed information hiding algorithm to carry secret message.



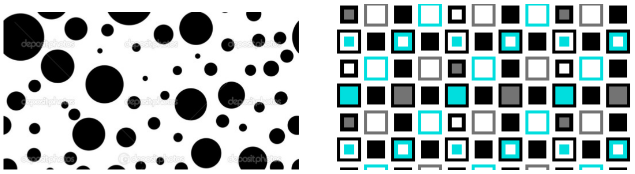
(a) Leaf Pattern Image[20] (b) Gaming Icon Pattern Image[21]

Fig. 4. Example pattern images from Internet with various position

If there is total number of n elements in a row, these elements can be permuted in n^n distinct positions (i.e., assuming that repetition is allowed). Therefore, each row of pattern image should be able to carry $\lfloor \log_2 n^n \rfloor$ bits of secret information in binary form. For instance, by using **Fig. 4(a)** as example, if there is 14 elements in a row, this row of elements in this case is able to produce 14^{14} positions. For this particular row, $\lfloor \log_2 14^{14} \rfloor = 53$ secret bits can be embedded.

3.2. Sizes

Other than position information, size is also one of the properties observed in pattern images. **Fig. 5(a)** and **Fig. 5(b)** are pattern images consist of elements with various sizes downloaded from the Internet. In information hiding algorithm, different sizes can be utilized to represent different set of binary secret information.



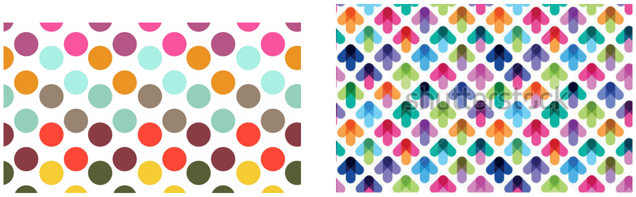
(a) Circle Pattern Image[22] (b) Square Pattern Image[23]

Fig. 5. Example pattern images from Internet with various sizes

For instance, **Fig. 5(a)** has circles with 8 different sizes. Each circle can be utilized to carry $\lfloor \log_2 8 \rfloor = 3$ bits of binary information, i.e., 000, 001, ... 111. Similar information hiding concept can be applied to other pattern images which consist of elements of various sizes.

3.3. Colors

Color is also one of the important properties in synthesizing pattern image. Colorful pattern image can be utilized as background of design or independently as an image to serve as painting, wallpaper, household design, etc.



(a) Color Dots Pattern Image[24] (b) Color Arrows Pattern Image[25]

Fig. 6. Example pattern images from Internet with various colors

Fig. 6(a) and **Fig. 6(b)** shows two colorful pattern images downloaded from the Internet. In information hiding algorithm, various colors can be used to carry binary information. For instance, if there are total number of 16 color variants in **Fig. 6(b)**, $\lfloor \log_2 16 \rfloor = 4$ bits of information (i.e., 0000, 0001, 0010, ... 1111) can be represented by each colored element to synthesis a pattern image similar to the shown figure.

3.4. Others

In this paper, we only discussed three important properties in synthesizing pattern images, including position, color and size. There are other contributing properties in synthesizing pattern images such as direction, transparency, shape, etc., which can also be utilized in proposed information hiding concept to carry information. Besides, combination of various properties can also be used to increase the embedding capacity and also strengthen the security of the embedded images.

Fig. 7 shows the flow of proposed decoding process. The embedded image will be fed into the data extraction algorithm to extract the embedded secret. Decoding pseudo-code in the data extraction algorithm is depending on the properties which were discussed earlier in this section.

4. EXPERIMENTAL RESULTS

4.1. Experimental Setup

In this experiment, a simple prototype is built to synthesis pattern image for comparison and discussion purposes. This simple prototype utilizes color as the main property to carry secret information.

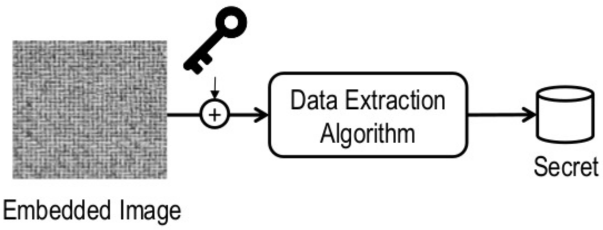


Fig. 7. Proposed Decoding Process

4.2. Output Image

In this subsection, output image from the prototype will be added for side-by-side comparison with the other pattern images downloaded from the Internet. All pattern images are shown in **Fig. 8** for visual comparison purposes.

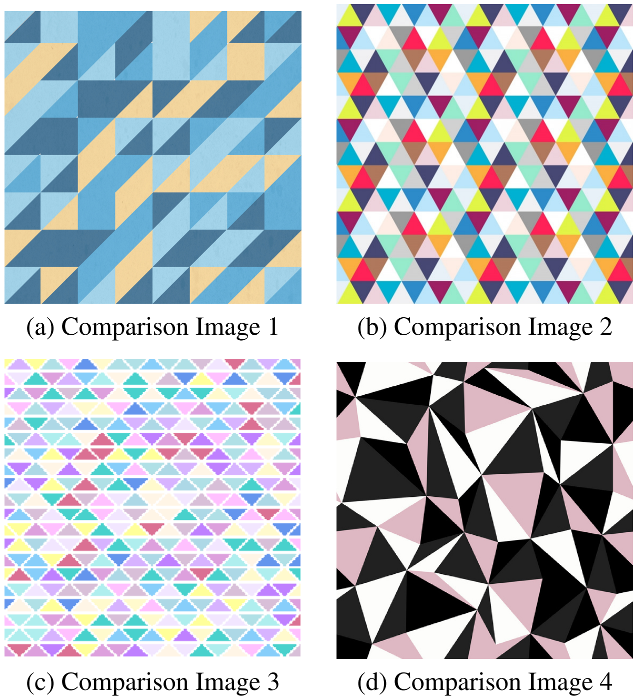

(a) Comparison Image 1
(b) Comparison Image 2
(c) Comparison Image 3
(d) Comparison Image 4

Fig. 8. Visual comparison of output image from prototype and pattern images downloaded from the Internet

By examining the pattern images visually, it is very difficult to distinguish between output image generated by proposed prototype and other images downloaded from the Internet. In fact, the output image generated by proposed prototype with secret information is shown in **Fig. 8(c)**.

4.3. Embedding Capacity

In the prototype, output image of 350×350 pixels are synthesized based on the predefined patterns (i.e., upward triangle and downward triangle), colors and secret message. The output image consists of 3 8-bits layers, which represent Red, Green, Blue color information, range from 0 to 255. As for the colors, the prototype utilizes 16 color codes, as indicated in **Table 1**.

Table 1. Color Codes utilized in Pattern Image Synthesis

No.	$\{R, G, B\}$	Secret Information
1	$\{255, 245, 230\}$	0000
2	$\{255, 250, 205\}$	0001
3	$\{255, 255, 153\}$	0010
4	$\{242, 230, 255\}$	0011
5	$\{215, 179, 255\}$	0100
6	$\{191, 128, 255\}$	0101
7	$\{175, 238, 238\}$	0110
8	$\{176, 224, 230\}$	0111
9	$\{72, 209, 204\}$	1000
10	$\{216, 191, 216\}$	1001
11	$\{255, 192, 293\}$	1010
12	$\{219, 112, 147\}$	1011
13	$\{221, 160, 221\}$	1100
14	$\{173, 216, 230\}$	1101
15	$\{135, 206, 250\}$	1110
16	$\{100, 149, 237\}$	1111

In the encoding process, after receiving secret information as an input, the secret information will be first encrypted using the key, K_1. Then, the encrypted secret information will be converted into binary format and grouped into non-overlapping 4 bits block. The color will then be assigned to this particular block in filling the triangle pattern by using the color representation as shown in **Table 1**.

In this prototype, the embedding capacity available is 4480 bits as there is only 1120 triangles to be filled with the colors. The decoding process is the reverse procedures of the encoding process as described earlier by using the same K_1.

5. DISCUSSION

5.1. Statistical and Comparison Attacks

In terms of statistical attack, there is no modification on the LSB or pixel values of the image, which leaves no trace of statistical changes available. All the colors in pattern image should be equally distributed to serve the perceptual appearance purposes, therefore, statistical attack cannot be applied to the proposed method. As for comparison attack, there is no cover image utilized in our proposed technique. Hence, comparison attack between cover image and output image also cannot be applied to the proposed method.

5.2. Visual Image Quality

In our proposed prototype, 16 color codes are carefully selected to ensure the harmonization within the colors in the synthesized pattern image. The properties (e.g., color, size, position) and choice of elements within the property (e.g., choice of colors, sizes and positions) should be carefully chosen to not arouse the suspicious of the attackers.

5.3. Enhancing Embedding Capacity

The output image generated by the prototype of size 350×350 can only used to accommodate 4480 bits of secret information. More embedding capacity can be added if more color codes are utilized. For instance, 32 color codes can be utilized to embed 5 bits of information per color element.

Besides, combination of different properties also can be explored to enhance the embedding capacity, such as color and size, color and position, size and position, etc. More permutation in synthesized pattern image can enables more embedding capacity.

6. CONCLUSION

In conclusion, this paper proposed a novel information hiding technique without using cover medium. In the proposed technique, secret information is utilized as the input to synthesis pattern image. Three properties in pattern image can be utilized as the basis of the image synthesis, including size, color and position. Simple prototype is developed to proof the proposed concept and discuss the feasibility of the proposed technique in terms of avoidance of attacks, visual image quality and embedding capacity.

7. REFERENCES

[1] Chi-Kwong Chan and L.M. Cheng, “Hiding data in images by simple lsb substitution,” *Pattern Recognition*, vol. 37, no. 3, pp. 469 – 474, 2004.

[2] R. Chandramouli and N. Memon, “Analysis of lsb based image steganography techniques,” in *Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205)*, 2001, vol. 3, pp. 1019–1022 vol.3.

[3] X. Zhang, “Separable reversible data hiding in encrypted image,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, April 2012.

[4] N. Cvejic and T. Seppanen, “Increasing the capacity of lsb-based audio steganography,” in *2002 IEEE Workshop on Multimedia Signal Processing.*, Dec 2002, pp. 336–338.

[5] P. Yadav, N. Mishra, and S. Sharma, “A secure video steganography with encryption based on lsb technique,” in *2013 IEEE International Conference on Computational Intelligence and Computing Research*, Dec 2013, pp. 1–5.

[6] Zhicheng Ni, Y. Q. Shi, N. Ansari, and Wei Su, “Reversible data hiding,” in *Circuits and Systems, 2003. ISCAS ’03. Proceedings of the 2003 International Symposium on*, May 2003, vol. 2, pp. II–912–II–915 vol.2.

[7] X. Li, B. Li, B. Yang, and T. Zeng, “General framework to histogram-shifting-based reversible data hiding,” *IEEE Transactions on Image Processing*, vol. 22, no. 6, pp. 2181–2191, June 2013.

[8] Zhibin Pan, Sen Hu, Xiaoxiao Ma, and Lingfei Wang, “Reversible data hiding based on local histogram shifting with multilayer embedding,” *Journal of Visual Communication and Image Representation*, vol. 31, pp. 64 – 74, 2015.

[9] Hao-Tian Wu, Shaohua Tang, Jiwu Huang, and Yun-Qing Shi, “A novel reversible data hiding method with image contrast enhancement,” *Signal Processing: Image Communication*, vol. 62, pp. 64 – 73, 2018.

[10] M. Arabzadeh, M. S. Helfroush, H. Danyali, and K. Kasiri, “Reversible watermarking based on generalized histogram shifting,” in *2011 18th IEEE International Conference on Image Processing*, Sept 2011, pp. 2741–2744.

[11] Jun Tian, “Reversible data embedding using a difference expansion,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, Aug 2003.

[12] D. M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721–730, March 2007.

[13] D. M. Thodi and J. J. Rodriguez, “Reversible watermarking by prediction-error expansion,” in *6th IEEE Southwest Symposium on Image Analysis and Interpretation, 2004.*, March 2004, pp. 21–25.

[14] X. Li, B. Yang, and T. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” *IEEE Transactions on Image Processing*, vol. 20, no. 12, pp. 3524–3533, Dec 2011.

[15] Ming Chen, Zhenyong Chen, Xiao Zeng, and Zhang Xiong, “Reversible data hiding using additive prediction-error expansion,” in *Proceedings of the 11th ACM Workshop on Multimedia and Security*, New York, NY, USA, 2009, MM&#38;Sec ’09, pp. 19–24, ACM.

[16] Xinlu Gui, Xiaolong Li, and Bin Yang, "A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding," *Signal Processing*, vol. 98, pp. 370 – 380, 2014.

[17] Andreas Westfeld and Andreas Pfitzmann, "Attacks on steganographic systems," in *Information Hiding*, Andreas Pfitzmann, Ed., Berlin, Heidelberg, 2000, pp. 61–76, Springer Berlin Heidelberg.

[18] K. Wu and C. Wang, "Steganography using reversible texture synthesis," *IEEE Transactions on Image Processing*, vol. 24, no. 1, pp. 130–139, Jan 2015.

[19] Zhenxing Qian, Hang Zhou, Weiming Zhang, and Xinpeng Zhang, "Robust steganography using texture synthesis," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, Jeng-Shyang Pan, Pei-Wei Tsai, and Hsiang-Cheh Huang, Eds., Cham, 2017, pp. 25–33, Springer International Publishing.

[20] "Leaf icon pattern background by vecteezy," `https://www.vecteezy.com/vector-art/104014-leaf-icon-pattern-background`, Accessed: 2018-2-11.

[21] "Gaming pattern background by andrey pavlychev," `https://dribbble.com/shots/563689-Icons-Pattern`, Accessed: 2018-2-11.

[22] "Circle pattern image by new design life," `http://www.newdesignfile.com/post_vector-circle-pattern_65497/`, Accessed: 2018-2-11.

[23] "Background pattern by emoticons wallpaper," `http://www.emoticonswallpapers.com/background-background-pattern-039-2062-14.html`, Accessed: 2018-2-11.

[24] "Dotted pattern background by public domain pictures," `http://www.publicdomainpictures.net/view-image.php?image=147442&picture=dotted-pattern-background`, Accessed: 2018-2-11.

[25] "Seamless pattern from color arrows by shutterstock," `https://www.shutterstock.com/image-vector/seamless-pattern-color-arrows-143348623?src=rV8lDNBmVVTp1CMHfqvEsA-1-7`, Accessed: 2018-2-11.