26th Conference Radioelektronika 2016, April 19-20, Košice, Slovak Republic

Image steganography with using QR code and cryptography

Vladimír Hajduk[1], Martin Broda[1], Ondrej Kováč[2], Dušan Levický[1]

[1]Dept. of Electronics and Multimedia Communications, [2]Dept. of Technologies and Electronics, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic

vladimir.hajduk@tuke.sk, martin.broda@tuke.sk, ondrej.kovac@tuke.sk, dusan.levicky@tuke.sk

ABSTRACT

This paper is focused on proposal of image steganographic method that is able to embedding of encoded secret message using Quick Response Code (QR) code into image data. Discrete Wavelet Transformation (DWT) domain is used for the embedding of QR code, while embedding process is additionally protected by Advanced Encryption Standard (AES) cipher algorithm. In addition, typical characteristics of QR code was broken using the encryption, therefore it makes the method more secure. The aim of this paper is design of image steganographic method with high secure level and high non-perceptibility level. The relation between security and capacity of the method was improved by special compression of QR code before the embedding process. Efficiency of the proposed method was measured by Peak Signal-to-Noise Ratio (PSNR) and achieved results were compared with other steganographic tools.

Index Terms— steganography, DWT, QR code, image, secret message

1. INTRODUCTION

Image steganography, the secret embedding of message into digital images, is represented to protection possibility of confidential information. Image steganographic methods include these principles of covert embedding. First one is based on modification Least Significant Bit (LSB) [1]. The LSB steganalytic methods have advantage of simple encode and guaranteed successful decoding if image is unchanged by noise or attacks. In these methods, LSB of the image pixels are replaced with the bits of message, while the pixels of the cover image are chosen either sequentially or randomly. Luo et al. [2] have proposed the LSB matching method, where the data is hidden in the edges.

The other category of image steganography is based on modification of transformation coefficients. Discrete Cosine Transformation (DCT) and DWT are common used techniques to gain that coefficients from an input image. Very popular tool based on modification of specific transformation coefficients is F5 [3]. Specifically Haar Discrete Wavelet Transformation (HDWT) is utilized by Chan et al. s´ method [4] to transform cover image from spatial to frequency domain. In additional, high frequency coefficients are compressed by Huffman (or arithmetic) coding method. Lin [5] proposed the method that is connected with a reversible data hiding scheme based on the varieties of image DCT coefficients.

Other information hiding technique is based on spread spectrum steganography [6]. As suggested by the name, the message is spread, and then is added to cover data. Further hiding method in static images include statistical steganography. Principle of algorithms in this category is preserving of statistical image features after embedding of secret message.

Some of the methods, mainly if the secret information is embedded in the text form, consider image color model. Such method which enables conversion between RGB and YC_bC_r color model without information loss was proposed in [7].

On the other hand, there are different methods of steganalysis. Steganalysis is utilized to detect the subliminal channels established by steganography. These methods are based on the strong complex mathematical calculations. Classifier is the main part of such tools and an efficiency of steganalytic methods is also dependent on a type of classifier [8, 9].

2. DISCRETE WAVELET TRANSFORMATION

The DCT which is frequently used in the field of image processing has two main drawbacks.

The first one is that the DCT does not provide any integer output hence the spectral coefficients are needed to be quantized. From the theory, it is well known that the quantization is always connected with the loss of information. In this case this loss is represented by quantization noise.

The second one is that in the DCT image pixels are processed by blocks. In practice it is possible to talk about

The paper was supported by Ministry of Education of Slovak Republic VEGA Grant No. 1/0075/15.

978-1-5090-1674-7/16/$31.00 ©2016 IEEE

blocks with a size 8×8 pixels. On the site of synthesis, a combination of quantization and segmentation leads to appearance of the disturb artefacts and the PSNR is decreased.

These drawbacks can be eliminated by use of the Integer Discrete Wavelet Transformation (IDWT). The difference between the IDWT and DWT is that the IDWT does not use convolution between input sequence and impulse response of filter [10]. The IDWT is also known as lifting implementation (L) DWT, it uses only operations of prediction, correction, summation and rounding. One decomposition stage of the LDWT for biorthogonal bank of filters BF (5,3) is shown in Fig. 1.

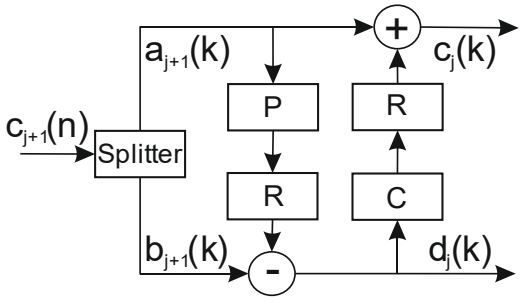

Fig. 1 One decomposition stage of LDWT

The decomposition coefficients are acquired from the input sequence as follows. The input sequence of samples $c_{j+1}(n)$ is divided in even $b_{j+1}(k)$ and odd $a_{j+1}(k)$ samples into two branches. On the base of the odd sequence, samples of the even sequence are predicted by the predictor P. These predictions are subtracted from the even sequence. Thus the sequence of detail coefficients $d_j(k)$ is created. From $d_j(k)$ corrections are acquired by the corrector C. These corrections are summed together with the sequence $b_{j+1}(k)$ and the approximation sequence $c_j(k)$ is acquired. From Fig. 1 it is clear that values of the correction and prediction are rounded. By the rounding R, the integer output of the LDWT is achieved. It is clear that the recovered sequence $c_{j+1}(n)$ is not influenced by the rounding on the side of a synthesis. The sequences $c_j(k)$ and $d_j(k)$ are given by the following Eq. (1, 2).

$$d_j(k) = b_{j+1}(k) - \left\lfloor \frac{1}{2}\left[a_{j+1}(k) + a_{j+1}(k+1)\right] \right\rfloor \quad (1)$$

$$c_j(k) = a_{j+1}(k) + \left\lfloor \frac{1}{4}\left[d_j(k-1) + d_j(k)\right] \right\rfloor \quad (2)$$

The backward transformation is simply realized by reordering operations of the prediction, correction and summation. By using properties of the separated transformation core, two dimensional (2D) transformation is achieved by the 1D LDWT (Fig. 1) which is at first applied on rows of the input image [11]. This leads to a creation of two subimages. In the next step these subimages are decomposed by the 1D LDWT applied on columns and the final decomposition, consisting of four subimages, is created. Block diagram of the 2D LDWT is shown in Fig. 2.

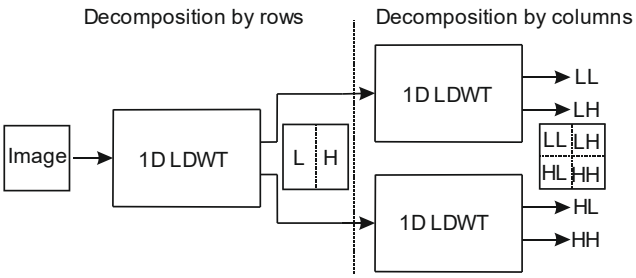

Fig. 2 Implementation of 2D LDWT by 1D LDWT connected into the cascade

3. PROPOSED IMAGE STEGANOGRAPHIC METHOD

The image data are used as cover medium in the proposed method and the secret message is defined by QR code. The QR code can code different types of input data (numeric, alphanumeric and binary). In the proposed method, QR code can be compressed due to different sizes of module. The higher size of the module is important so that QR code can be read from the higher distance. On the other hand, there are some redundant bits in the each module which can be effectively reduced without loss of information before the embedding process. This compression is very useful knowing that embedding process could be successful even if the input QR code is bigger than modified area. Subsequently, QR code included the secret message is encrypted using AES and it is embedded into the DWT subimages of the cover medium.

3.1 QR code

QR code is the trademark for a type of matrix barcode (or two-dimensional barcode). Four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) are used to efficiently store data. A QR code is consisting of the black square modules arranged in a square grid on a white background. QR code can be read by an imaging device (such as a camera, scanner, etc.) and processed using Reed–Solomon error correction until the image can be appropriately interpreted.

The amount of data that can be stored in the QR code symbol depends on the datatype (mode, or input character set), version (1, 2, …, 40, indicating the overall dimensions of the symbol), and error correction level. There are four error correction levels (level L - 7%, M - 15%, Q - 25% and H - 30% of codewords can be restored) indicating measure

of possible disruption of QR code what is can be still read using the imaging devices. The standard square module width can be different. The larger a module is the more stable and easier to read with a QR Code scanner it becomes.

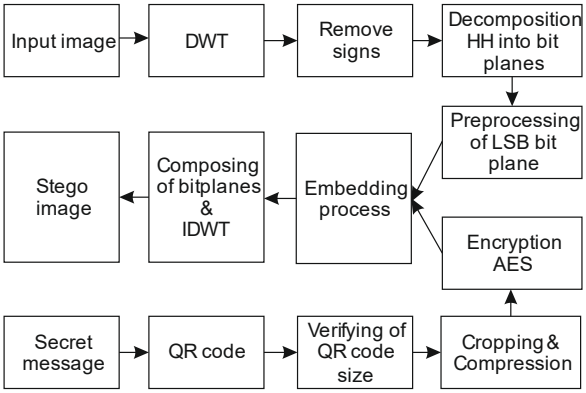

Fig. 3 Block diagram of proposed image steganographic method

3.2 Embedding process

Embedding process of secret message in form of QR code into static image is implemented by these steps (the block diagram is illustrated in Fig. 3):

1) Loading input data, image and QR code.
2) Verifying of QR code size.
3) Cropping of white space from QR code (four bits from every side). Subsequently, each module of same adjacent bits in the QR code is replaced by one bit with specific value from this module in order to compression of QR code. The size of module depends on the user option. This step is illustrated in Fig. 4.
4) Obtaining of cropped QR code size. This size information will be inserted into transformation coefficients of image as first.
5) Input image is transformed into LDWT domain by Haar wavelets (four subimages LL, LH, HL, HH).
6) Determine the size of subimage HH, where is embedded secret message.
7) The signs of specific transformation coefficients are stored in sign matrix.
8) Subsequently, the signs of transformation coefficients are removed and subimage HH is decomposed into 8 bit planes.
9) QR code embedding is performed in LSB bit plane of HH subimage, where LSB bits are replaced by encrypted bits of QR code. Bit substitution is implemented from third row and second column of matrix HH because of preservation of statistical features of image.
10) After embedding, modified LSB bit plane is composed into HH subimage.
11) Inverse DWT is applied on modified subimage HH and original HL, LL a LH subimages.
12) After implementation of these steps, stego images with embedded secret message in form of QR code is created.

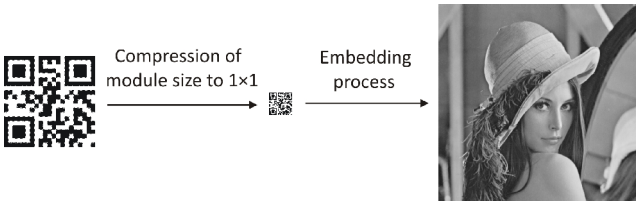

Fig. 4 Compression of module size

3.3 Extraction process

Secret message in form of QR code can be obtained from stego image by extraction algorithm of proposed steganographic method. This process is based on inversion operations considering embedding algorithm. Finally, obtained QR code can be read by an imaging device (i.e. smartphone), where a secret message in text or data form is acquired.

4. EXPERIMENTAL RESULTS

The proposed method was verified by objective quality measure PSNR for different versions of QR code. The PSNR values was obtained by comparison cover and stego versions of three well-known images (Lena, Baboon and Barbara) illustrated in Fig. 5.

Fig. 5 Tested cover images (Lena, Barbara and Baboon)

The number of characters coded by QR code is dependent not only on version of QR code, but also on data type. The maximum storage capacities for different data types and for the highest level of QR code (version 40, error correction level L) is illustrated in TABLE I.

TABLE I. MAXIMUM STORAGE CAPACITIES OF QR CODE (VERSION 40)

Input data	Max. characters	bits/char	Possible characters
Numeric only	7089	3,3	0,1,2…9
Alphanumeric	4296	5,5	0–9, A–Z, space, $, %, *, +, -, ., /, :
Binary/Byte	2953	8	ISO 8859-1

Experimental results show, that PSNR of our proposed method attain higher values providing using QR code with higher capacity. These results are illustrated in TABLE II, where there is shown dependence of PSNR on the size (version) of secret message in form of QR code. In the article, there were verified three versions of QR code (version 1, version 20 and version 40) with default error correction level (level L) and with the size of module 4×4 bits. The size of secret message in binary form for verified version of QR code are as follows: 136 bits (version 1), 6864 bits (version 20) and 23624 bits (version 40).

TABLE II. PSNR VALUES OF STEGO IMAGES FOR PROPOSED STEGANOGRAPHIC METHOD

Image	Version of QR code	Size of QR code	PSNR [dB]
Lena (512×512)	1	84×84	71.38
	20	388×388	59.48
	40	708×708	54.33
Barbara (512×512)	1	84×84	71.11
	20	388×388	59.42
	40	708×708	54.32
Baboon (512×512)	1	84×84	71.44
	20	388×388	59.46
	40	708×708	54.31

The main advantage of our proposed steganographic method is compression of the module size in the QR code before embedding process. After this step, input QR code with arbitrary size of the module can be embedded into the same area.

The proposed method was compared with other steganographic tools described in [2], [4] and [6]. Our proposed method can be easily modified for embedding also into the next subimages or the next bit planes (LSB and MSB - 7th bit planes), whereby embedding capacity can be increased. In this experiment, QR code was embedded into 7th and 8th bit plane of LDWT subimages HH, HL, LH. The comparison of PSNR and embedding capacity with other tools is illustrated in TABLE III.

TABLE III. COMPARISON OF OUR PROPOSED METHOD WITH OTHER STEGANOGRAPHIC TOOLS

		Our method	Chan et al. [4]	Luo et al. [2]	Lin [5]
Lena (512×512)	PSNR [dB]	50.24	37.23	38.8	37.7
	Capacity [kbits]	141.744	99.947	66.064	129.791

In the TABLE III there is shown that embedding capacity 141744 bits is achieved by upper described modified method for QR code of version 40 with L error correction level, whereas PSNR between cover and stego image (Lena) was 50.24 dB. Better results of PSNR are achieved by the proposed method in comparison to the other verified tools for the same or even higher embedding capacity.

5. CONCLUSION

In this paper, we proposed image steganography tool with using LDWT (Haar wavelet) and QR coding. Improvement of security was performed by AES ciphering of QR code. The advantage of the method is compression of the module size in the QR code before embedding process. The aim of our research was to compare our proposed method with other image steganographic tools with regards to imperceptibility of embedded secret message and embedding capacity. The results show that PSNR of proposed method achieves higher values as compared tools for the same or very similar capacity.

6. REFERENCES

[1] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, Kluwer Academic Publisher, 2001.

[2] W. Luo, F. Huang, J. Huang, "Edge adaptive image steganography based on LSB matching revisited," IEEE Trans Inform Forensics Secure, 5 (2) (2010), pp. 201–214.

[3] A. Westfeld, "High capacity despite better steganalysis (F5 – a steganographic algorithm)," In I. S. Moskowitz, Information Hiding, 4th International Workshop, vol. 2137, New York: Springer-Verlag, pp. 289-302 (2001).

[4] Y. K. Chan, at. al., "A HDWT-based reversible data hiding method," J Syst Softw, 82 (2009), pp. 411–421.

[5] Y. K. Lin, "High capacity reversible data hiding scheme based up on discrete cosine transformation," J Syst Softw, 85 (2012), pp. 2395–2404.

[6] L. Marvel, C. Boncelet, C. Retter, Spread spectrum image steganography, IEEE Transactions on Image Processing 8, 1999, pp. 1075–1083.

[7] M. Broda, V. Hajduk, D. Levický, "Image steganography based on combination of YCbCr color model and DWT," in ELMAR, 2015 57th International Symposium, pp. 201-204, 28-30 Sept. 2015.

[8] M. Broda, V. Hajduk, D. Levický, "The Comparison of Classifiers in Image Steganalysis," Acta Electrotechnika et Informatica, FEI-TU: Košice, 2014, vol. 14, no. 4, pp. 1-4, ISSN 1335-8243.

[9] V. Bánoci – M. Broda – G. Bugár – D. Levický, "Universal Image Steganalytic Method", In: Radioengineering, December 2014, Volume 23, Number 4, pp. 1213-1220. ISSN 1210-2512.

[10] T. Acharya, C. Chakrabarti, "A survey on lifting-based discrete wavelet transform architectures," Journal of VLSI signal processing systems for signal, image and video technology, vol. 42, no. 3, 321-339, 2006.

[11] O. Kováč, J. Mihalík, "Lossless encoding of 3D human head model textures," Acta Electrotechnica et Informatica. vol. 15, no. 3, 2015.