DWT Steganography with Usage of Scrambling

Jakub Oravec
Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics
University of Technology Košice
Košice, Slovakia
jakub.oravec@tuke.sk

Ján Turán, Ľuboš Ovseník
Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics
University of Technology Košice
Košice, Slovakia
jan.turan@tuke.sk, lubos.ovsenik@tuke.sk

***Abstract*—This article describes image steganography technique, which uses Discrete Wavelet Transform and Standard map for storage of secret data in form of binary image. Modifications, which are done on cover image depend on its scrambled and decomposed version. To avoid unnecessary amount of changes, proposed approach marks location of altered DWT coefficients. The paper ends with illustration of yielded results and presents some possible topics for future work.**

***Keywords*—chaotic maps, Discrete Wavelet Transform, Standard map, steganography**

I. Introduction

Steganography is one of possible ways for securing communication between two users. Unlike cryptography, it does not rely on hiding the content of sent data, but it tries to make the exchange of messages undetectable. This is possible by masking the secret communication with performing of another one – the visible one is used as a cover.

Computer images are quite frequently used as covers for hidden communication. Most of images, which are being sent nowadays, contain large amounts of pixels. The color shade for each of those pixels is given by combination of certain number of bits. Some changes in these bits can store information, such as it is done by the *LSB* (Least Significant Bit) approach [1, 2].

Current state of steganographic techniques which use images can be summarized in two groups of techniques. First group contains algorithms which try to reduce the impact of changes done in cover image. The cost of changes is calculated prior to embedding of secret data. Second group of approaches use algorithms, which were created without consideration of their possible detection. These techniques could be called *naive* [3]. For ensuring higher level of security, it is possible to use naive techniques in combination with one of encryption standards, such as *AES* (Advanced Encryption Standard) [4].

However, conventional encryption standards have some properties, which are not desirable in steganographic applications. One example is present on Fig. 1. In this case, the image was processed by AES in *ECB* (Electronic CodeBook) mode – it was encrypted as set of non-overlapping pixel blocks. As we can see, if image pixel intensity values are not different enough, the edges of original image content can be seen also after the encryption.

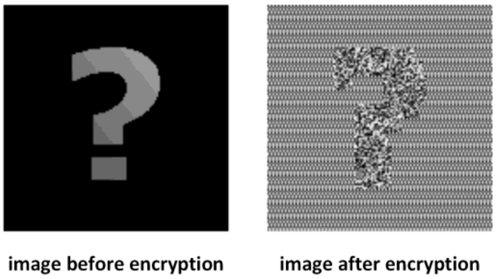

Fig. 1. Example of image encrypted by AES in ECB mode

Not all encryption algorithms have mentioned disadvantage. Examples can be found in group of so-called *chaotic maps*. Most of these maps process images in *square* blocks (with resolution of *nxn* pixels). Size of the blocks is arbitrary. If image, which should be encrypted has square resolution, whole image could be processed as one block.

Encryption by means of chaotic maps can yield another advantage – the choice of modified pixels in cover image depends on selected map. The map can also use several parameters, however their transmission between sending and receiving side directly violates main principle of steganography – to send data without recognition of other users.

The rest of this paper is organized as it follows: the second chapter deals with description of used techniques. Solution for mentioned problems is included in chapter three. Fourth chapter verifies the theory with simple experiments and provides their results. After that, the advantages and drawbacks of proposed approach are presented in fifth and last chapter.

II. Used Techniques

A. *Discrete Wavelet Transform (DWT)*

DWT and its inverse version are used for providing domain for embedding, or extraction of secret data in form of binary image. The goal of DWT is decomposition of original signal to multiple subbands. The number of these depends on level of decomposition and amount of signal dimensions. In case of images, which are two dimensional, the decomposition of first level produces four subbands – *cA*, *cH*, *cV* and *cD*. The first one is considered to be an approximation of the original image, other three contain horizontal, vertical and diagonal details.

Computation of DWT for two dimensional signals exploits fact that DWT is separable. At first values from image rows are used in computations, and after that the calculations are carried out on columns of values provided by previous step.

Calculations performed during the decomposition could be represented by passing the original image to a filter bank. The bank uses pairs of Quadrature Mirror Filters in each level of decomposition. Approximation subband (in selected direction) is yielded as output of low-pass filter, while the detail subband is created by passing signal through high-pass filter. Steps and resulting subbands of first level decomposition with usage of *Haar* wavelet for two dimensional signal are shown on Fig. 2. Image reconstruction is analogous to decomposition.

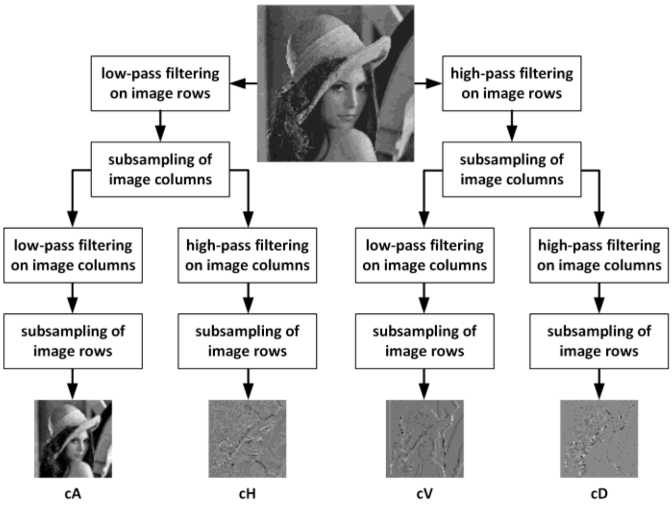
low-pass filtering on image rows
high-pass filtering on image rows
subsampling of image columns
subsampling of image columns
low-pass filtering on image columns
high-pass filtering on image columns
low-pass filtering on image columns
high-pass filtering on image columns
subsampling of image rows
subsampling of image rows
subsampling of image rows
subsampling of image rows
cA
cH
cV
cD

Fig. 2. Image decomposed by first level of DWT with Haar wavelet

Subsampling is possible due to fact that filtered signal has exactly half the frequencies of signal prior to filtering. Because of Nyquist's theorem and possibility of perfect reconstruction, the decimation is done with factor of two. Reconstruction uses opposite operation, interpolation with the same factor.

Usage of Haar wavelets provides one interesting feature. Values of coefficients in subbands are either *integer* or *half-integer* numbers. Examples of half-integers could be 0.5, 2.5 or -1.5. This property, and also the *sign* of coefficients can be used for storing information in DWT domain [5].

B. Standard Map (StM)

StM is one of chaotic maps, which operates with two values [6, 7]. Number of these values enables usage of StM in field of image encryption – it can be used for *scrambling* (rearrangement) of image pixels. In this case the intensity values are not changed. Result of scrambling depends on number of used iterations. After each iteration, the scrambled image becomes input for next iteration.

Set of equations for discrete version (computations with integers) of StM is denoted as (1):

$$x_{i+1} = x_i + y_i \ (mod\ n), \qquad (1)$$
$$y_{i+1} = y_i + K.round(sin\ (2\pi.\ x_{i+1})/n)\ (mod\ n),$$

where x_{i+1} and y_{i+1} are coordinates of $i+1^{st}$ iteration, x_i and y_i are coordinates of i^{th} iteration, x_{i+1}, y_{i+1}, x_i and $y_i = 0, 1, ..., n\text{-}1$. Value of n denotes height and width of input image and $K = 0, 1, ..., n\text{-}1$ is parameter of the map. Rounding operation in second equation is needed for calculations with integers.

The presence of n in set of equations (1) is necessary for achieving property of area-preserving [7]. Maps with this feature do not create images with different resolutions after their iterations. However, this property limits resolutions of input images – they have to be square (nxn pixels). This limitation can be overcome by creating multiple rectangular selections from non-rectangular image.

An example of image after certain iterations of StM is shown on Fig. 3. In this case the value of parameter K is equal to $n/2 = 64$.

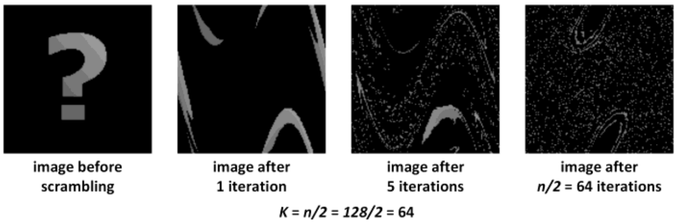

Fig. 3. Scrambling of image pixels done by StM

Due to limited amount of possible pixel locations, chaotic maps usually show some signs of *periodicity*. Period for selected pair of chaotic map and input image can be calculated by creating orbits for each image pixel. The principles of period computation for other chaotic map, Arnold's cat map are described in detail in [8].

Reconstruction of original image after performed chaotic mapping can be done in two ways. First is iterating the image until period of map is reached. Second approach uses inverse set of equations, which are in case of StM denoted as (2):

$$y_i = y_{i+1} - K.round(sin\ (2\pi.\ x_{i+1})/n)\ (mod\ n), \qquad (2)$$
$$x_i = x_{i+1} - y_i\ (mod\ n).$$

III. Proposed Solution

For enabling the possibility of hidden communication, our approach uses two algorithms. First one is the embedding algorithm, second one is used for extraction of secret data. Both these algorithms try to decrease the impact of secret data embedding by marking the *location* of pixels, which are modified.

Embedding algorithm can be divided into several steps. At first the cover image is decomposed by first level of DWT with Haar wavelet. When subbands are acquired, their coefficients are rounded to nearest half-integers. Coefficients of subbands are then scrambled using StM. The ones from *cD* subband are used for storing the location of secret data. After that the embedding of data takes place. At this point, inverse scrambling on subbands is performed. Last step is reconstruction of stego image from subbands.

Extraction starts with decomposition of stego image by first level of DWT with Haar wavelet. Coefficients are rounded to nearest half-integer and they are scrambled by StM. After that the position of secret data and also their content is extracted.

A. Scrambling done by StM

Scrambling operations, which take place enable embedding of secret data into pixels with pseudo-random locations. StM uses *round(n/2)* iterations and parameter *K* has the same value. The values could have been entered as keys, however our approach uses only stego image for extraction of secret data.

The usage of StM requires square cover image which produces square matrices with subband coefficients. If subband matrices are not square, algorithm chooses largest possible square selections.

B. Marking the position of embedded secret data

Some steganographic techniques use all possible locations for embedding of secret data. In the case that image with secret data has smaller resolution than the maximal embedding capacity of cover enables, the first one could be padded [5, 9, 10]. The embedding of padding causes same changes as embedding of secret data. Bigger amount of changes can negatively affect performance of steganographic algorithm. This is the reason, why proposed approach tries to minimize the number of modified coefficients by selection and marking of embedded secret data position.

The marking itself is done by flipping the signs of certain coefficients in scrambled version of *cD* subband. Amounts of rows and columns used for embedding of secret data are converted to binary words. These words have lengths of $ceil(log_2(h\text{-}1))$ and $ceil(log_2(w\text{-}1))$, where *h* and *w* are height and width of cover image. The flipping of signs takes place in first $ceil(log_2(w\text{-}1))$ coefficients in last row (for marking width of image with secret data) and in first $ceil(log_2(h\text{-}1))$ coefficients in last column (for marking height of image containing secret data). These locations for image with resolution of 8x8 pixels are shown on Fig. 4.

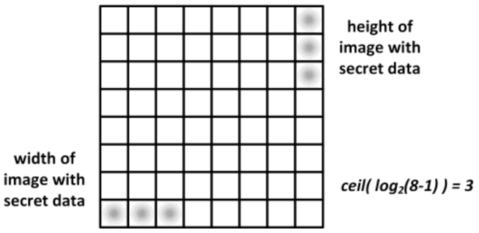
height of image with secret data
width of image with secret data
$ceil(\ log_2(8\text{-}1)\ ) = 3$

Fig. 4. Example of locations for position marking

Coefficients with desired locations are processed by following rules (3):

$$\begin{aligned} &if\ \ b == 1\ \ and\ \ c < 0\ \ then\ \ c' = -c,\\ &if\ \ b == 0\ \ and\ \ c > 0\ \ then\ \ c' = -c,\\ &if\ \ b == 0\ \ and\ \ c == 0\ \ then\ \ c' = -0.5, \end{aligned} \tag{3}$$

where *b* is bit from binary word denoting height or width of image with secret message, *c* is scrambled coefficient from *cD* subband which will be processed and *c'* is its new value.

The idea behind (3) is that *c'* is positive while *b* equals one, and it becomes negative for *b = 0*. Zero is considered to be positive, so third rule has to be applied for cases when both *b* and *c* are zero and negative value of *c'* is needed.

C. Modification of cover data

Maximal embedding capacity of proposed approach is limited to images with width *floor(w/2)* and height *floor(h/2)*, where *w* and *h* are width and height of cover image. This limitation is caused by properties of DWT with Haar wavelet – the changes made in one of subbands can affect values of coefficients in another subbands. Unwanted alterations like these can result in extraction of corrupted secret data.

Coefficients of scrambled subbands are preprocessed before embedding, or extraction of secret data. This step rounds values of coefficients to nearest half-integers (values of some coefficients could be distorted). After the rounding, the embedding, or extraction starts from top left corner of matrices with scrambled coefficients. For purpose of data hiding, the modification of coefficients follows algorithm (4):

```
if  $s(k, l) == 1$                                          (4)
    if  $cH(k, l) \geq 0$
            $cH(k, l) = floor(cH(k, l)) + 0.5;$
            $cV(k, l) = floor(cV(k, l)) - 0.5;$
    else
            $cH(k, l) = floor(cH(k, l)) - 0.5;$
            $cV(k, l) = floor(cV(k, l)) + 0.5;$
    end
else
    $cA(k, l) = ceil(cA(k, l)); cH(k, l) = floor(cH(k, l));$
    $cV(k, l) = ceil(cV(k, l)); cD(k, l) = floor(cD(k, l));$
end
```

where *s* is one of bits from binary image with secret data, *k* and *l* are pixel coordinates in this image, $k = 1, \ldots, w_s$, $l = 1, \ldots, h_s$, w_s and h_s are width and height of image with secret data, *cA*, *cH*, *cV* and *cD* are scrambled subbands of cover image.

Bits of secret data can be extracted from *cH* and *cV* subbands. If value of coefficient is half-integer, bit of secret data was equal to *1*, if it is integer, secret data bit was *0*.

Usage of maximal possible embedding capacity results in altering coefficients, which are used for storing the position of secret data. However, operations which are used in this approach allow errorless extraction of both position and secret data bits from the same coefficient.

IV. Experimental Results

Several experiments were carried out for verification of properties of proposed approach. All of them were conducted on PC with 2.5 GHz CPU and 12 GBs of RAM in software package Matlab.

The set of images, which was used in experiments is shown on Fig. 5. Cover images *lena*, *flowers* and *station* had resolution of 128x128 pixels, their color depth was 8 bits. Images with secret data were binary, with resolutions of 64x64 (*qstnmrk*) and 64x48 pixels (*secdata*).

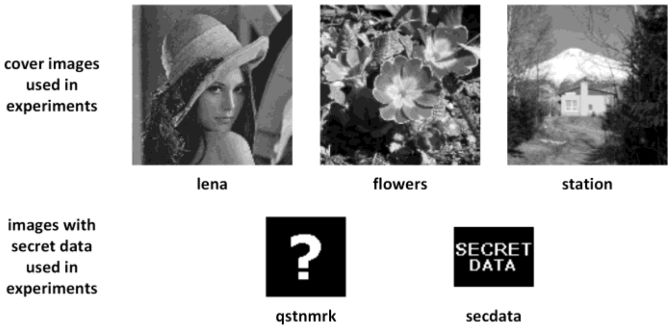
cover images used in experiments
lena
flowers
station
images with secret data used in experiments
?
SECRET DATA
qstnmrk
secdata

Fig. 5. Images used during experiments

Equations for calculation of parameter *PSNR* (Peak Signal to Noise Ratio), which is used for evaluating performance of proposed algorithm can be found in [1] or [3]. Computed values of PSNR are presented in TABLE I. Effects of embedding can be seen on Fig. 6.

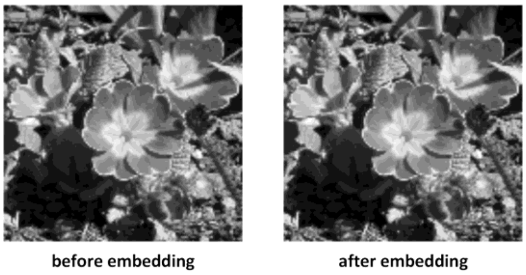

Fig. 6. Comparison of image before and after embedding

TABLE I. PEAK SIGNAL TO NOISE RATIO VALUES

PSNR$_{[dB]}$	***lena***	***flowers***	***station***
qstnmrk	56.005	54.4487	53.9809
secdata	56.9345	55.1442	56.4856

V. CONCLUSION

This paper proposes steganographic approach, which uses DWT and StM for hiding of secret data. This combination brings up the possibility of modifying various pixels of cover image. Another advantage is limitation of amount of altered DWT coefficients in case that maximal possible capacity of cover image is not reached. Also, application of StM can be considered as advancement to approach's security.

However, presented techniques also cause some drawbacks. Substitution algorithms can achieve higher capacity and sometimes also smaller distortion of used cover images. Marking of secret data position causes more alterations of cover image if maximal possible capacity is reached. These problems could be good topics for our future research.

ACKNOWLEDGMENT

This work was supported by research grant KEGA 006TUKE-4/2014.

REFERENCES

[1] J. Fridrich, Steganography in Digital Media: Principles, Algorithms and Applications. Cambridge: Cambridge University Press, 2009, pp. 60-64. ISBN: 978-0-52119-019-0.

[2] J. Oravec, J. Turán, Ľ. Ovseník, „LSB Steganography with Usage of Mojette Transform for Secret Image Scrambling“ in Proc. of 23rd Int. Conf. IWSSIP 2016. Bratislava (Slovakia), 2016, pp. 258-261. ISBN: 978-1-46739-554-0. DOI: 10.1109/IWSSIP.2016.7502754.

[3] D. Levický, Kryptografia v informačnej a sieťovej bezpečnosti (in Slovak). Košice: Elfa, 2012, pp. 81-92. ISBN: 978-8-08086-163-6.

[4] J. K. Saini, H. K. Verma, „A Hybrid Approach for Image Security by Combining Encryption and Steganography“ in Proc. of 2nd Int. Conf. ICIIP 2013. Waknaghat (India), 2013, pp. 607-611. ISBN: 978-1-46736-101-9. DOI: 10.1109/ICIIP.2013.6707665.

[5] V. Bánoci, G. Bugár, D. Levický, „A Novel Method of Image Steganography in DWT Domain“ in Proc. of 21st Int. Conf. Radioelektronika 2011. Brno (Czech Republic), 2011, pp. 1-4. ISBN: 978-1-61284-324-7. DOI: 10.1109/RADIOELEK.2011.5936455.

[6] B. Chirikov, Research Concerning the Theory of Non-Linear Resonance and Stochasticity. Geneva: CERN, 1971, pp. 45.

[7] J. Fridrich, „Symmetric Ciphers Based on Two-Dimensional Chaotic Maps“ in Int. J. of Bifurcation and Chaos, vol. 8, no. 6, pp. 1259-1284, June 1998. ISSN: 0218-1274. DOI: 10.1142/S021812749800098X.

[8] F. Svanström, Propeties of a generalized Arnold's discrete cat map. Diploma thesis, Linnaeus University (Sweden), 2014, 32 pp.

[9] G. Prabakaran, R. Bhavani, „A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform“ in Proc. of Int. Conf. ICCEET 2012. Nagercoil (India), 2012, pp. 1096-1100. ISBN: 978-1-46730-210-4. DOI: 10.1109/ICCEET.2012.6203811.

[10] A. Samčović, J. Turán, „Attacks on Digital Wavelet Image Watermarks“ in J. of Electrical Engineering, vol. 59, no. 3, pp. 131-138, 2008. ISSN: 1335-3632.

BIOGRAPHIES

Jakub Oravec (Ing.) is currently PhD. student at University of Technology, Košice (as of September 2016). His research interests include steganography and digital image processing.

Ján Turán (Dr. h. c., prof., RNDr., Ing., DrSc.) received Ing. (MSc.) degree with honours from the Czech Technical University, Prague, Czech Republic, in 1974, and RNDr. (MSc.) degree with honours from Charles University, Prague, Czech Republic, in 1980. He received a CSc. (PhD.) and DrSc. degrees in radioelectronics from University of Technology, Košice, Slovakia, in 1983, and 1992, respectively. Since March 1979, he has been at the University of Technology, Košice as Professor. His research interests include digital signal processing and fiber optics, communication and sensing.

Ľuboš Ovseník (doc., Ing., PhD.) received Ing. (MSc.) degree from the University of Technology, Košice, in 1990. He received PhD. degree in electronics from the same university in 2002. Since February 1997, he has been at the University of Technology, Košice as Associate Professor. His general research interests include optoelectronics, digital signal processing, fiber optic communications and fiber optic sensors.