Discrete Transformations and Noise-Resistant Coding of Still Images in Steganography Problems

Vladimir N. Kustov, Anatoly A. Kornienko, Dmitry K. Protsko

Department of Computer Science and Information Security,
Emperor Alexander I St. Petersburg State Transport University,
Saint Petersburg, Russia
kvnvika@mail.ru, kaa.pgups@yandex.ru

Boris V. Sokolov

Laboratory of Information Technologies in System Analysis and Modeling,
St. Petersburg Institute for Informatics and Automation of the RAS,
Saint Petersburg, Russia
sokolov_boris@inbox.ru

Abstract

This article is another attempt of a comprehensive solution in the field of steganography data transmission. We also consider software model prototype that fully implements the process of hidden messages transmission in digital photographs. All stages of hidden message processing on the whole way from the sender to the recipient are taken into account. The programming model uses a discrete wavelet transform and new hiding algorithms based on the «Arnold cat map» decomposition. The efficiency of using noise-resistant coding methods and multi-threshold decoding to ensure high probability of integrity and reliability of hidden messages when transmitting them through communication channels with a high level of noise is also shown.

Introduction

The following features can characterize the current state of research in the field of steganography:

- Extensive use of discrete transformations of digital still images used as containers for steganography message, and the need to combine the well-known methods of discrete signal conversion with simple, well-tested old algorithms.
- Development of more and more new methods of steganography, which provide high secrecy, confidentiality and reliability of message delivery.
- Increasingly more complete account of the characteristics of data transmission channels and interference arising in it, especially in the conditions of their high noise level.
- The need to develop and implement new, more advanced methods of noise-resistant coding of hidden messages transmitted over communication channels, to ensure their integrity.
- Development of new, simpler, faster and energy-efficient noise-resistant decoders that have characteristics close to the optimal decoders, but with linear (polynomial) time costs for the implementation of the decoding process.

These paper attempts of a comprehensive solution that takes into account the above features in one way or another, and presents a prototype of the software model for implementing the process of transmitting hidden messages in digital still images. Using discrete transformations of still images, new hiding algorithms and methods of noise-resistant coding to ensure a high probability of their integrity and reliability during transmission over communication channels with a high level of noise proposed.

1 Discrete Transformation of Still Images

Methods of image steganography can be divided into two groups: the first uses the spatial area of the image, the second - the frequency area. Methods that edit a spatial area directly affect the container itself (for example, changing image pixels). However, such methods are highly sensitive to various container changes: scale modification, rotation, cropping, adding noise or interference to the channel, various loss compression - are likely to destroy the hidden message.

Methods that allow messages to be embedded in the frequency domain first convert the container file and then only perform the embedding. These methods do not depend on image formats [Dav07], [Che08]. The information hiding the steganography methods is based on linear orthogonal transformations such as:

- Discrete Hadamard transform (DHT);
- Discrete Fourier transform (DFT);

In: B. V. Sokolov, A. D. Khomonenko, A. A. Bliudov (eds.): Selected Papers of the Workshop Computer Science and Engineering in the framework of the 5 th International Scientific-Methodical Conference "Problems of Mathematical and Natural-Scientific Training in Engineering Education", St.-Petersburg, Russia, 8–9 November, 2018, published at http://ceur-ws.org

- Discrete cosine transform (DCT);
- Discrete wavelet transform (DWT);
- Singular value decomposition (SVD).

Among all the discrete transformations, the most popular are the discrete cosine transform (DCT) [Kus17] and the discrete wavelet transforms (DWT). The prevalence of these methods is explained by their wide use for image compression. Especially successfully, they are used in JPEG and JPEG2000 standards. The JPEG standard uses the DCT and the DWT is used the JPEG2000 image compression standard.

In [Kus17], the authors have successfully shown the use of combined stegoalgorithm on the basis of the method of the Least Significant Bit (LSB) in combination with DCT (LSB & DCT). In this paper, the authors tried to use LSB in combination with DWT (LSB & DWT). Let us dwell on this.

2 Steganography System Model

The General model of the steganography system is shown in figure 1. In this model, a secret graphic digitized message in 24-bit bmp format is used as an embedded message (figure 2).

The choice of a graphical object as an embedded message was made due to its higher resistance to noise in transformations. One of the main blocks in this model of the steganography system is the block implementing the function of embedding presented in figure 3. Consider its functionality.

First, it is designed to perform DWT and embed a pre-converted hidden message into it.

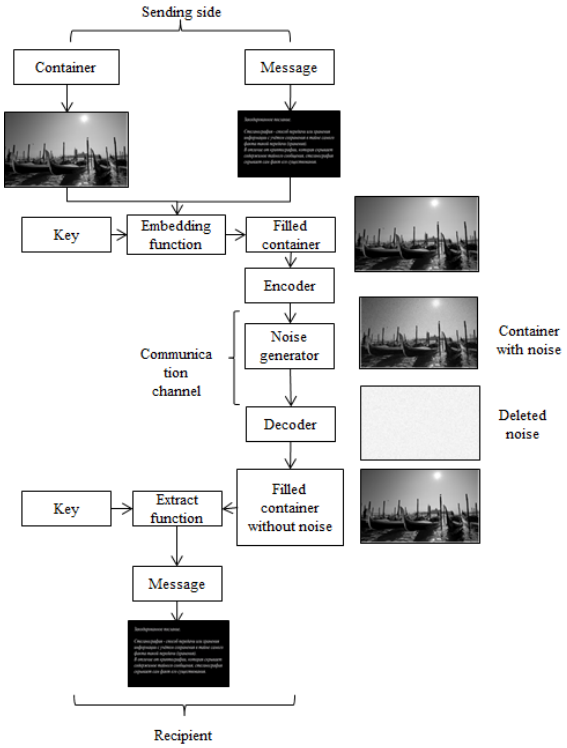


Figure 1: General Steganography System Model

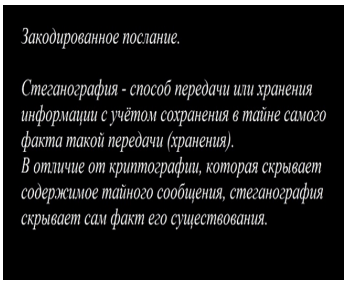


Figure 2: Embedded Message

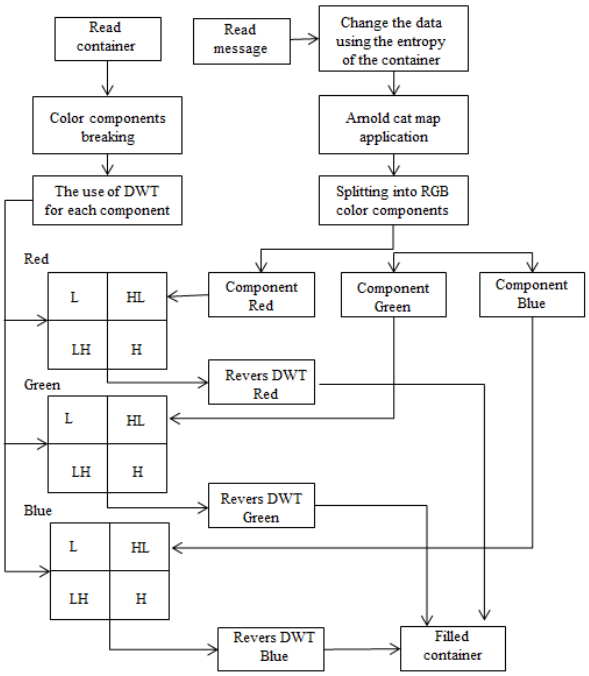
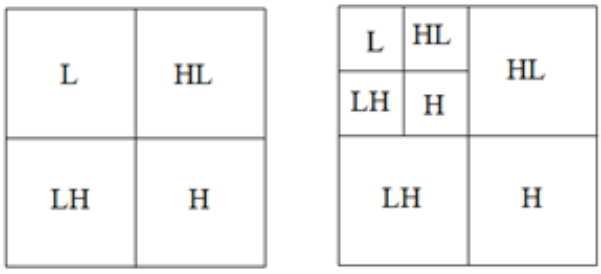


Figure 3: Embedding Function

For each decomposition level, first a DWT is performed in the vertical direction and then a DWT in the horizontal direction. After performing the first level of decomposition, we obtain a block 4x4, shown in figure 4a.

The next level of decomposition is performed in the low-frequency part obtained in the previous decomposition (figure 4b).



a) The first stage b) The second stage

Figure 4: Two DWT Stages

The main real indicators of concealing information methods in steganography are:

- PSNR-peak signal to noise ratio;
- Imbedded capacity;
- Correlation.

PSNR is inversely proportional to capacity and directly proportional to correlation and vice versa. During the study, the correct ratio of PSNR to capacity and correlation was found, which suggests that the information can be sent over an unprotected channel of information transmission, without fear of unauthorized access by a third party. But also keep in mind that the larger the imbedded message, the greater its impact on the steganography container and for big data, you must choose a larger container.

In the proposed approach, DWT is used to decompose the image into high frequency and low frequency subbands.

In turn, imbedded message converted using the Arnold cat map (ACM). In mathematics, ACM is identified with the chaotic mapping on the torus first proposed by Vladimir Arnold [Div11].

ACM can be viewed as a two-dimensional map described by relations:

$$p' = q\ (mod 1)$$

$$q' = p + 2q\ (mod 1).$$

In these relations, the dash sign shows the dynamics of parameter values change at the next time step. As the phase space of ACM typically consider the surface of a torus. The parameter p on the torus specifies the coordinates of the Parallels, and the parameter q is the coordinate along the Meridian of the torus. The range of values of both parameters is limited by the interval from zero to one. Typically, a unit square with p and q coordinates is used as a graphical representation of ACM. The name ACM is because Vladimir Arnold illustrated it in a picture resembling a cat's head (figure 5) [Div11].

The record of these relations in the matrix representation has the form:

$$\begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} \begin{vmatrix} p \\ q \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} \begin{vmatrix} p \\ q \end{vmatrix}.$$

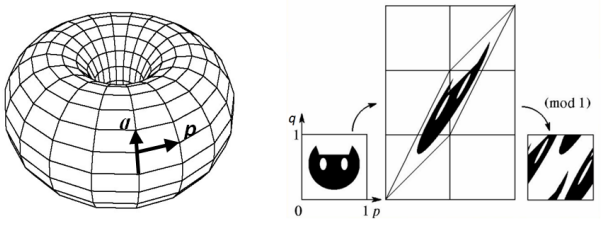


Figure 5: Graphical ACM Interpretation

It should be noted that any picture subjected to ACM (for example, the cat's head) always retains its area. It is also known that ACM is used to demonstrate the dynamics of chaotic processes (figure 6).

Also it should be noted that the ACM decomposition is iteratively reversible. Let us illustrate this fact by the example shown in figure 6. This figure shows that at a certain iteration step the image converted using ACM (in this case, the embedded message) necessarily takes the form of the original. In the example below, each picture has an iteration number corresponding to that picture. On iteration number 194 the image becomes equivalent to the original. Let's imagine that we used the original image as a hidden message, converting it to iteration number 50. Then when decoding this image to get the original message view, we need to perform 194-50 = 144 iterations! From here, we can conclude that the values 50 and 144 can be used as secret keys, respectively, at the stages of embedding and extracting the hidden message.

After the transformation is applied to the ACM algorithm, the hidden message is divided into RGB components, and embedded using LSB algorithm in the corresponding sub-band HL. After the implementation, the reverse DWT (RDWT) is applied, the components are assembled again and the filled stegocontainer is obtained in accordance with the embedding function (figure 3).

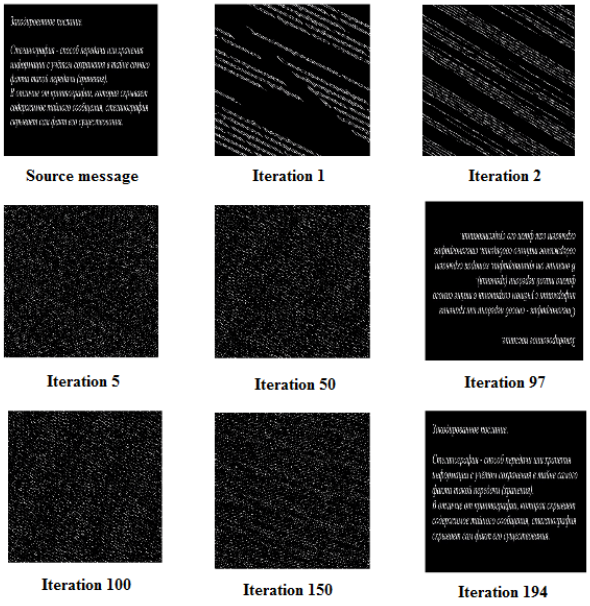


Figure 6: ACM Hidden Message Transformation

ACM in this combination is used to increase safety. It allows you to extract a full secret message only to the recipient who has information about the method of embedding (key). The filled container is sent to the communication channel (figure 1) after the application of noise-resistant coding, where it is exposed to noise generated by the noise generator.

A noisy hidden message after the decoding procedure is passed to the input of the block that implements the extraction function (figure 1). The function of extracting a hidden message is performed in the following order. The DWT is first performed (similar to that shown in

figure 3) applied to the filled steganography container passed an error-correcting decoding. Then, the LSB reverse conversion is extracted from the HL blocks and the RGB components of the secret message are assembled together. Gathered secret message in turn subjected to reverse ACM (RACM) using the key for the stage of extracting secret message and acquiring complete, is delivered to the recipient. If necessary, the empty container is assembled by applying a reverse DWT (RDWT) transformation to its RGB components and connecting them into a single unit.

Let us perform statistical analysis of the effectiveness of the developed stego-algorithm. Peak signal to noise ratio (PSNR) means the ratio between the maximum possible signal value and the noise power that distorts the signal

values [Ami10]. This metric is used to show the difference between empty and filled containers:

$$PSNR = 10\,lg\left(\frac{255^2}{MSE}\right).$$

The root mean square error (MSE) – determines the difference between the intensities of the filled and empty containers:

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(f(i,j) - (f'(i,j)))^2.$$

Where *f(i,j)* is an empty container and *f'(i,j)* is a filled container. A large MSE value indicates that the original image is of poor quality, and Vice versa.

Capacity is the relation of the hidden message size to container size. It is calculated by the formula:

$$\text{Capacity} = \frac{\text{hidden message pixels number}}{\text{container pixels number}}.$$

Correlation used to display a linear relationship between empty and filled containers [Mut11]:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{(n-1)s_x s_y}.$$

Table 1 presents the main performance indicators of this algorithm. As can be seen from the table, the proposed method copes with hiding data in the image.

Table 1: The Main Performance Indicators

N	Container size MxN	Message size	Empty container PSNR	Filled container PSNR	Correlation	Capacity
1	1680 x 1050	635 x 715	45.0553	15.2341	0.9997	0.29
2	1440 x 990	635 x 715	47.8423	20.4323	0.9998	0.26
3	1360 x 768	600 x 400	49.3421	12.2342	0.9997	0.22

3 Error-correcting Codes and Multi-threshold Decoding

Of particular relevance in the transmission of hidden messages through channels of communication with interference is the use of noise-resistant coding.

Recently, in the field of digital signal transmission in channels with a high level of noise, methods of noise-correcting coding based on the use of multi-threshold decoders (MTD) of self-orthogonal codes (SOC) are intensively used. The prototype of MTD is a simple decoder of Massey [Mas69]. New technical solutions used in the MTD represent the implementation of an effective algorithm of noise-correcting coding. Distinctive features of MTD are:

- Linear computational complexity;
- High efficiency of error correction;
- Iterative error correction process that constantly brings the decoding process closer to the optimal decoder;
- Easy technical implementation;
- Ability to work efficiently with different code speeds in high-interference channels;
- High performance and significant energy gain.

Let us consider in more detail the device of MTD [Zol12]. An example of a multi-threshold character block coder (MTBC) scheme for a self-orthogonal code with one information branch is shown in figure 7. It can be seen that the encoder consists only of a shift register and a group of adders modulo q, where q=256.

In this example, the group of adders determined in accordance with the image of the polynomial $P=x^0+x^1+x^4+x^8$.

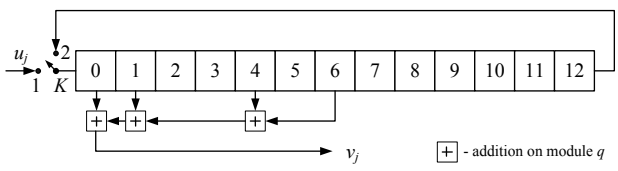


Figure 7: MTBC with One Information Branch

The scheme of the multi-threshold character block decoder (MTCBD) for such code has the form shown in figure 8. The information register performs the role of the

information branch here, and the role of the verification branch is the syndrome register.

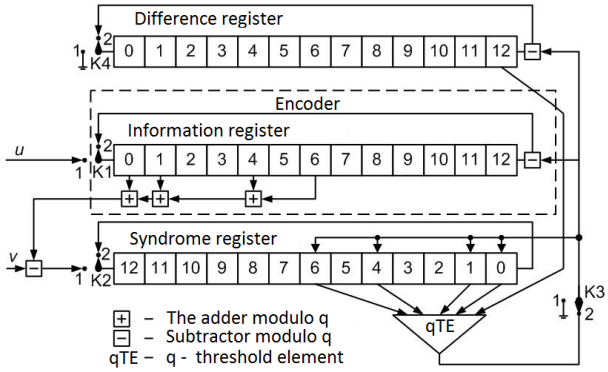


Figure 8: MTCBD with One Information and One Verification Branch

The MTCBD scheme consists only of shift registers, adders, subtracts modulo q and a threshold element (TE).

TE task is to count the most common characters in the corresponding positions of the syndrome and difference registers. For example, the symbol q1 occurs a1 times, and the symbol q2 occurs b1 times. Then, the value of |a1 – b1| compare with some set threshold value in the majority element with further correction of the associated elements in case of exceeding the threshold value.

An example of the MTBC scheme with two information branches presented in figure 9.

Table 2: Simulation results

q=256
volume =100000
P_{0_low}=0.25000
P_{0_high}=0.15000
P_{0_step}=0.00500

The parameters of the communication channel:
q- synchronous channel

The parameters non-binary coder
Number of information branches: nk=4
Number of test branches: nr=4
Number of possible symbol values: q= 256
Code rate: R=0.50

Code distance: 9
Code length: 9704
Number of decoding iterations: 7
The probability of error in the channel: P_0=0.16000
Number of blocks transmitted = 21
Number of information characters transmitted = 101892

Simulation results

The number of the iteration:
0 1 2 3 4 5 6 7
Number of errors at the output of different decoding iterations:
16347 14338 7384 259 0 0 0 0
Probability of error at the output of different decoding iterations:
1.60e-001 1.41e-001 7.25e-002 2.54e-003 0.00e+000 0.00e+000 0.00e+000 0.00e+000
The probability of an error on the symbol at the output of a non-binary decoder was 9.81e-006
The probability of an error on the block at the output of a non-binary decoder was 0.00e+000

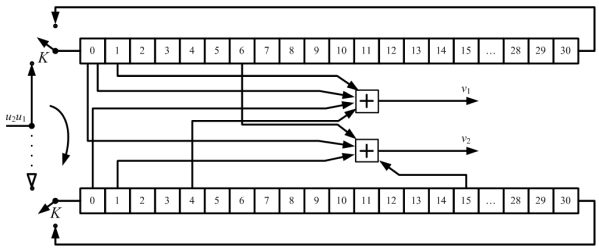


Figure 9: MTBC Scheme with 2 Information Branches

The simulation was carried out with the help of MTCBD, which has 4 information and 4 verification branches. The output file of the simulation results contained information on the simulation parameters, the encoder and decoder used in the simulation, as well as information on the estimated error probability at the output of the MTCBD and the number of errors remaining after decoding iteration for each error probability in the communication channel. An example of a typical entry in the results file is shown in table 2. As can be seen in table 2, the MTCBD is very effective. Given a sufficiently high probability of error in the channel 0.16 (16 decibels) and the size of the source character file consisting of 101892 characters (bytes), combined into 21 blocks, all errors, the total number of which in the source file was 16347, were eliminated at the fourth iteration.

A binary synchronous communication channel (BSC) with an independent error stream (channel without memory) subject to Gauss distribution was chosen as a communication channel model.

Let us consider the results of the stenographic process modeling as a whole using the model shown in figure 1.

Figure 10 shows a 24-bit BMP graphic file used as a steganography container.

Figure 10: Steganography Container

Figure 11: Steganography Container Are at the BSC Exit

After the function, embedding secret message, filled stegocontainer are supplied to MTCBC, and after the encoding process is transmitted in noisy BSC. The output of the BSC file has the form shown in figure 11.

From the output of the BSC stegocontainer are supplied to the MTCBD where all the noise is removed, and the file stegocontainer are taking on the appearance it had at the entrance to the BSC.

Filtered noise is shown in figure 12.

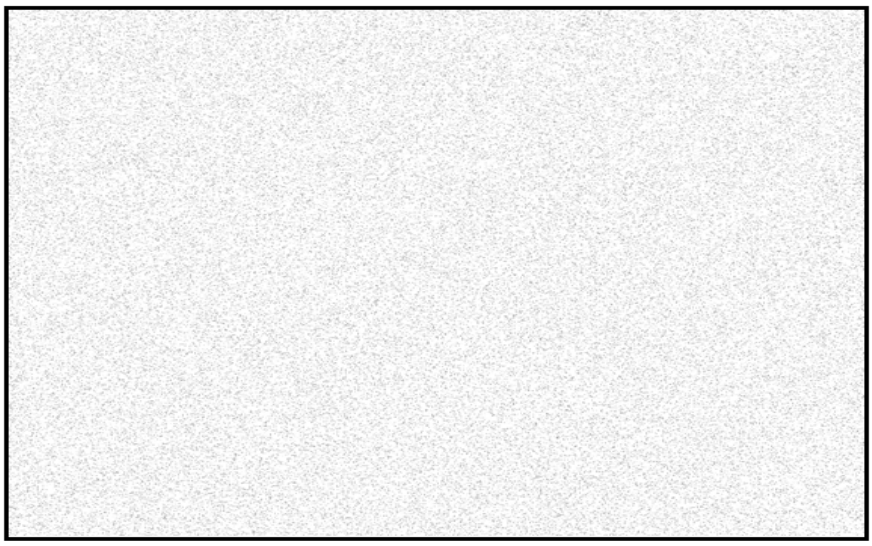


Figure 12: Filtered Noise

Output MTCBD the steganography container are supplied to the removal unit, the output of which then issued a secret message.

The following parameters were set for the final simulation:

- The code rate is 0.5;
- The probability of error in channel P0 = 0.25;
- Container size - 93640 bytes;
- Number of generated errors - 23543;
- Number of decoding iterations until all errors are fully retrieved - 18;

- Type of communication channel - BSC.

Conclusion

In the opinion of the authors, this paper describes a successful attempt of a comprehensive solution in the field of steganography container data transmission. The authors present a prototype of a software model based on four main components:

- Discrete wavelet transformation the steganography container are;
- Pre-coding the hidden message using Arnold's cat decomposition;
- Embedding encoded message on LSB algorithm in wavelet transformations the stegocontainer are;
- Application of noise-resistant coding in the communication channel using advanced technologies of multi-threshold decoding using MTD (multi-threaded decoder).

Conventionally, this combination of four components can be designated as DWT & ACM & LSB & MTD.

The authors believe that this model fully implements the process of transmission of hidden messages in digital still images. The model takes into account and agrees on the features of all processing hidden message stages.

Acknowledgments

Studies carried out on this topic were carried out with partial financial support from RFBR grants (No. 16-29-09482-ofi-m), under the budget theme No. 0073–2019–0004.

References

[Mes66] Messi John. Threshold decoding / Per. with English. Ed. by E. L. Bloch. M.: Mir, 1966.

[Zol12] Zolotarev V. V., Zubarev Y. B., Ovechkin G. V. multi-Threshold decoders and optimization theory of coding. M.: Hotline-Telecom, 2012.

[Kus17] Kustov, V. N., Protsko D. K. A Software model of steganography on the basis of a combination of methods LSB and DCT. Science and education in the XXI century. Collection of scientific papers on the materials of the international scientific-practical conference on February 28, 2017. Part 3. Tambov: LLC "Ucom Consulting company", 2017. P. 54-61.

[Dav07] David Frith," Steganography Approaches, Options and Implications", Network Security, August 2007.

[Che08] Cheddad A., Condell J., Curran K. and Mc Kevitt, P. (2008). Biometric Inspired Digital Image Steganography. Proc of the 15th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'08). P. 159-168.

[Div11] Divya Saxena," Digital Watermarking Algorithm based on Singular Value Decomposition and Arnold Transform", International Journal of Electronics and Computer Science Engineering (IJECSE), Vol. 1, No. 1, 2011, P. 22-27.

[Ami10] R. Amirtharajan, R. Akila, P. Deepika Chowdavarapu, "Comparative Analysis of Image Steganography", International Journal of Computer Applications, volume 2 – No.3, May 2010.

[Mut11] S. K. Muttoo, Sushil Kumar, "A mulltilayred secure, robust and high capacity image steganographic algorithm", 2011.

[Mas69] J. L. Massey, Shift-register synthesis and BCH decoding, IEEE Trans. Information Theory, IT-15 (1969), P. 122-127.