Scientific Research Publishing

Journal of Information Security, 2019, 10, 117-129
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform

Ashraful Tauhid[1], Maisha Tasnim[1], Saima Arifin Noor[1], Nuruzzaman Faruqui[2], Mohammad Abu Yousuf[2]

[1]Information & Communication Engineering, Bangladesh University of Professionals, Dhaka, Bangladesh
[2]Institute of Information Technology, Jahangirnagar University, Dhaka, Bangladesh
Email: ashtauhid@gmail.com, mtasnim0113@gmail.com, saimanoor1212@gmail.com, faruquizaman27@gmail.com, yousuf@juniv.edu

How to cite this paper: Tauhid, A., Tasnim, M., Noor, S.A., Faruqui, N. and Yousuf, M.A. (2019) A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform. *Journal of Information Security*, **10**, 117-129.
https://doi.org/10.4236/jis.2019.103007

Received: March 19, 2019
Accepted: June 29, 2019
Published: July 2, 2019

Abstract

Cryptography and Steganography are two prominent techniques to obtain secure communication over the shared media like the Internet. Steganography is slightly ahead of cryptography because of its stealthy characteristics. In this paper, a new method has been proposed which combines cryptography and steganography to ensure even more secure communication. The Advanced Encryption Standard (AES) in spatial domain of the carrier/cover image and Least Significant Bit (LSB) replacement in the transformed domain of the same image has been used after performing a Discrete Cosine Transform (DCT) on the pixels. An additional layer of security has been introduced by applying XOR operation on the AES encrypted message with the pixel values of the carrier image. The Peak Signal to Noise Ratio (PSNR) of the proposed algorithm is better than most of the similar algorithms. With better PSNR, the proposed method depicts a three layer of security of the information and error free decryption.

Keywords

Cryptography, Steganography, Security, Encryption, Decryption

1. Introduction

Modern lives have been taken over by technology and so is the information sharing media. Internet plays a key role in modern communication. Zillions of data like web browsing, emails, online transactions, social networking, audio & video files, etc. are being shared over the Internet. This transmission of data

makes the information vulnerable while they are up on the internet. Therefore, intruders like hackers can get an easy access to the shared information. So, data security is a primary concern in digital communications. Data security means that the data is to be protected from the unauthorized access and error introduction throughout the lifecycle. There are three practices that can ensure data security which are key management, data encryption, and tokenization. This security can be ensured by changing the information bits in such a fashion so that once the information bits are in the communication medium, they do not make any sense to the intruder while they get the access to the data but at the same time they can be reconfigured to the original information at the expected receiver's side. This idea can be sketched as a black-box for the time being. This black box takes the information bits as inputs and changes them to some other form and sends it to the receiver. The inverse black-box at the receiver's side will find the exact information bits from the changed form. This black-box is basically cryptography. The security parameters of cryptography are enhanced to a great extent by steganography. So, both cryptography and steganography can be used as the black-box for the overall data sharing systems. Cryptography basically conceals the actual message using a mathematical definition which can also be inversed to get the concealed data back. In steganography, the idea of information sharing is non-existent, *i.e.* the intruders will not even know that the information is being sent over the internet or some other information sharing medium. This is done by hiding the information in some kind of digital carriers like images, audios, videos and even protocols [1]. These carriers are also called cover media or cover object and after embedding the information into the cover media they are named as stego media or stego object [2]. The performance and efficiency of a steganography algorithm are measured using some important parameters which are imperceptibility, data embedding capacity, robustness, secrecy and accuracy [2].

In this paper, we represented a potential tri-layered secure image steganography using Advanced Encryption Standard (AES) technique as the cryptographic tool in the spatial domain of the image and also LSB replacements in the Discrete Cosine Transform (DCT) coefficients of the frequency domain. In the middle of these two operations there is also an XOR operation between the binary representation of the AES encrypted message and the pixel values of the image to ensure the security of the message even before passing to the frequency domain. With all these security measures the proposed algorithm suggests a good robustness and secrecy. Because of the transformed domain the imperceptibility is also ensured throughout the procedure with a decent data embedding capacity and accuracy.

The rest of the paper is organized as follows. In Section 2, the related works in the same or related fields are discussed. Section 3 sheds some light on the theoretical background of the work. Section 4 explains the proposed algorithm whereas Section 5 represents the results and the analysis of the experiments. Finally, the paper is concluded in Section 6.

2. Related Works

Steganography is extensively segregated into five different categories [3]. The categories are based on text, image, audio, video and network or protocol. Image is popular in steganography because of its surplus availability and redundancy. Two types of domain for information embedding in an image are mentioned and these are spatial domain embedding and frequency domain embedding [4]. There are quite a few techniques used to hide information in spatial domain. LSB substitution is one of the easiest and popular techniques used by different algorithms. LSB substitution is of two types; LSB replacement and LSB matching [5]. To embed by using LSB replacement method, we replace an LSB with bits of secret information in each pixel of the cover image [6]. In LSB matching, if the least significant bit of a byte in the cover image does not match with the next bit of the secret message, then the pixel bit of the cover is either increased or decreased by one, except at the boundary values [7].

Wu *et al.* proposed Pixel Value Difference (PVD), an embedding technique which embeds secret message into a cover image by amending the difference value of adjacent pixels pairs [8]. With 256 gray-valued Lenna as cover image, PSNR value of 48.43 dB was obtained by their method. An uneven embedding in PVD creates unusual steps in the histogram of pixel difference in the stage image which reveals the presence of hidden message. IPVD, an improved technique exploited this vulnerability [9]. A steganalyst can further estimate the number of embedded bits after detecting the steps in the histogram. So, the original PVD method is still vulnerable to the histogram analysis.

BPCS steganographic technique by Kawaguchi *et al.* made proper use of a characteristic of human visual system *i.e.* it cannot perceive the shape-information of too-complicated visual pattern [10]. Maya *et al.* proposed an algorithm to embed data based on BPCS and IWT and obtained a PSNR value of 37.70 dB for maximum hiding capacity [11].

Bansal *et al.* proposed an algorithm called shield algorithm using LSB replacement in the DCT values of the pixels and obtained a PSNR of 29.77 dB [12]. Jameelah, H.S. proposed an algorithm to hide an image within another image taken as the cover image which resulted in a PSNR value of 54.81 dB [13]. Gunjal *et al.* proposed a technique of steganography using blowfish algorithm and LSB replacement in the DCT coefficients of the image and obtained a PSNR of 72.75 dB [14]. Tseng *et al.* proposed a method using JPEG images and applied DCT to get the DC coefficients [15]. They used Quantization Error Table (QET) to track down less erroneous DC values and embed the information in their LSB. Their experimental results came out with a PSNR value of 47.92 dB at best. Hashad *et al.* proposed a robust steganography technique using LSB replacement in DCT coefficients [16]. They traced the message bit one by one in the 4-MSB of every byte and the positions were converted into coding map for encryption. They also used a positive integer "ρ" for further modification of the algorithm. Seivi *et al.* proposed a new technique of steganography based on edge detection

[17]. The shaper edges are first figured out and then LSB replacement is applied on the binary of the selected edge values. Banik *et al.* came up with an algorithm that hides secret messages scrambled according to Arnold Transform into the modified DCT coefficients and achieved a PSNR value of 47.17 dB [18].

Based on PSNR values, all of these papers suggest a decent security of the information transmission. The proposed algorithm worked on the PSNR value and came up with a better PSNR value than the methods discussed here. The results and comparisons with some other methods are discussed in Section 5.

3. Theoretical Backgrounds

In this section, we briefly introduce the theoretic background to develop the proposed method: Advance Encryption Standard (AES), Least Significant Bit (LSB) replacement and Discrete Cosine Transform (DCT).

3.1. Advance Encryption Standard

Advance Encryption Standard (AES) is an encryption algorithm which is widely used to ensure data security, integrity and privacy when transmitted through internet. AES has a block length and cipher key length of 128 bits whereas Rijndael has a minimum of 128 bits and maximum 256 bits. AES is a round based, symmetric block cipher cryptography algorithm which replaced DES for being extremely secure and for its excellent performance.

AES has an initial key addition round denoted by AddRoundKey, then N_{r-1} number of transformation rounds and a final round at the end. The input for N_r round including AddRoundKey is State and Round key. Three stages in AES are as follows [19]:

1) AddRoundKey Transformation Round

2) N_{r-1} rounds each composed of 4 transformation rounds

a) SubBytes Transformation

b) Shift Rows Transformation

c) Mix Columns Transformation

d) Add Round Key Transformation

3) A Final Round composed of

a) SubBytes Transformation

b) Shift Rows Transformation

c) Add Round Key Transformation

3.2. LSB Replacement

Images are stored and displayed digitally using binary digits or bits and each of the bits carries a portion of the total information [20]. The left-most bit is the Most Significant Bit (MSB) and right-most bit is the Least Significant Bit (LSB) of a byte. MSB contains most of the information whereas LSB contains least information. So apparently, any changes brought to LSB will cause less distortion to the image. This simple yet magnificent principle is used in image steganogra-

phy to hide information in cover image. The LSB of each of the pixel values of a cover image is replaced by the message bits and hence the message is hidden without significantly distorting the cover image. **Figure 1** is an illustration of the LSB replacement technique.

3.3. Discrete Cosine Transform

Discrete Cosine Transform (DCT) is very much alike Discrete Fourier Transform (DFT) [21]. DCT deals only with the real part or cosine part of DFT. Since image is a signal which doesn't contain any complex value so, DCT is used instead of DFT to convert the spatial domain to frequency domain. The equation (1) is the general equation for 1D-DCT.

$$C(u)=\left(\frac{2}{N}\right)^{\frac{1}{2}} a(u)\sum_{i=0}^{N-1} f(i)\cdot\cos\frac{(2i+1)u\pi}{2N} \tag{1}$$

Since, image is a 2D signal hence it requires two successive 1D DCT to find the 2D DCT values. Equation (2) is the general equation for 2D-DCT.

$$C(u,v)=\left(\frac{2}{N}\right)^{\frac{1}{2}}\cdot\left(\frac{2}{N}\right)^{\frac{1}{2}} a(u)a(v)\sum_{I=0}^{N-1}\sum_{i=0}^{N-I} f(i,j)\cdot\cos\frac{(2i+1)u\pi}{2N}\cdot\cos\frac{(2j+1)v\pi}{2N} \tag{2}$$

where, $a(u),a(v)=\begin{Bmatrix}\frac{1}{\sqrt{2}} \text{ for } u,v=0\\ 1, \text{otherwise}\end{Bmatrix}$

$f(i,j)$ is the intensity of the pixel in row i and column j.

$C(u,v)$ is the DCT coefficient in row u_i and v_j of the DCT matrix.

4. Proposed Method

The proposed method combined AES, LSB replacement and DCT altogether to improve the data security. First the secret message is encrypted using AES Cryptography algorithm which generates a cipher text. The cipher text after

1	0	1	0	1	1	0	0	0	1	1	1	0	1	1	0

(a) 2 bytes of cover image

1	0

(b) 2 bits of message

1	0	1	0	1	1	0	1	0	1	1	1	0	1	1	0

(c) LSB replacement technique

Figure 1. Illustration of LSB replacement technique in cover image.

being represented in binary is XORed with the pixel values of the grayscale cover image, which generates a modified encrypted message. This step increases data security even more. At the same time, we extracted DCT coefficients of the cover using DCT transformation and converted them into binary. The modified encrypted message is then inserted in the LSB position of the DCT coefficients of grayscale cover image by LSB replacement method which creates DCT coefficients of grayscale stego-image. At last stego-image is obtained after performing IDCT on the binary representation of stego-image's DCT coefficients. Figure 2 illustrates the embedding procedure of the proposed method at the sender's end. Information embedding algorithm is illustrated in Algorithm 1.

This stego-image is sent to its destination through public network. At the destination, to get back the original secret message from the stego-image, modified cipher text is extracted from it. Modified cipher text, when XORed with the pixel values of grayscale cover image, generates cipher text. Next the cipher text is decrypted using AES decryption method using the same cipher key used in the sender's side. In this way secret message is reopened by the recipient in the destination. Figure 3 illustrates the extracting procedure of the proposed method at the receiver end. Information extracting algorithm is illustrated in Algorithm 2.

5. Experimental Results and Analysis

To carry out the experiments of the proposed algorithm, color images and grayscale images of different formats were used as the cover image. The color images are converted into grayscale image before doing the image operations. Table 1 demonstrated the specification of the images those were used as cover images for experimental purposes. The hidden message which is embedded in cover image is:

"Starting believing is the first stage of getting succeeded and true soldiers never back off from a fight, they just take some time to regroup. And remember, when you see people running, don't you dare to keep up with their pace. Take time, have patience and walk your road. You might find shortcuts."

To prove the efficacy of the proposed method we have considered both subjective and objective evaluation. In subjective evaluation, stego-image quality is measured by visual inspection. In objective evaluation, various metrics like

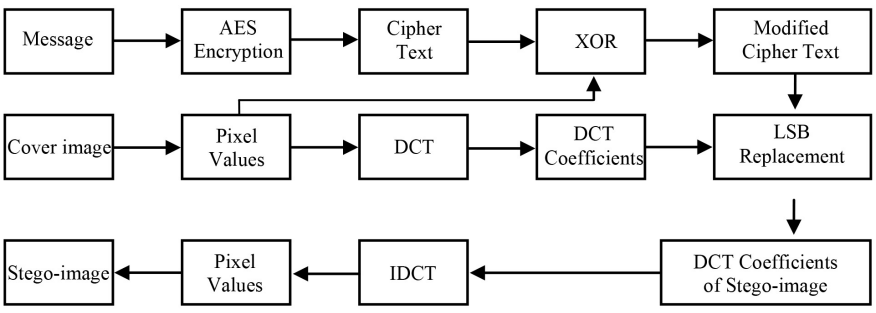

Figure 2. Embedding block diagram.

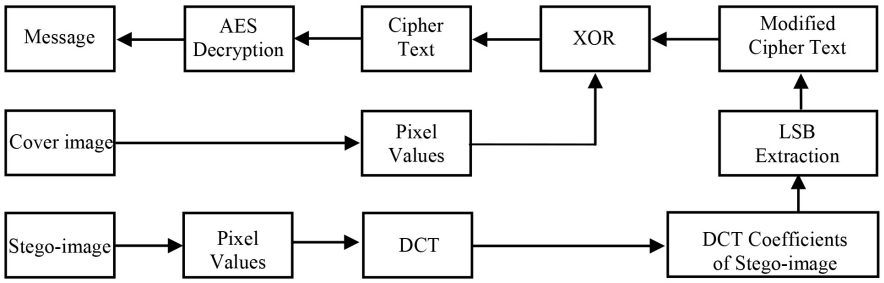

Figure 3. Extracting block diagram.

Algorithm 1. Information embedding algorithm.

Input: Message M, Cover image I_c
Output: Embedded stego-image I_s
Initialization: Read I_c
***Preprocessing of M*:**
Read M
Apply AES encryption to get cipher text, C_t
Binarize C_t
***Preprocessing of I_c*:**
Resize I_c to a square matrix of pixel values P_{ij}
Divide I_c into 8 × 8 blocks
Apply DCT in each block, P_{uv}
Generate an 8 × 8 quantization table, Q_t
Quantize each block by P_{uv}/Q_t and round them, Q_{uv}
Find DC values by $Q_{uv} \leftarrow Q_{uv}((u*8)-7,(v*8)-7)$ and binarize
***Embedding in LSB*:**
Modified cipher text, $M_c \leftarrow C_t \oplus P_{ij}$
for each Q_{uv}
Q'_{uv} : = Embed M_c replacing LSBs of Q_{uv}
end for
Apply inverse DCT in Q'_{uv}
Reconstruct the image

Algorithm 2. Information extracting algorithm.

Input: Stego-image I_s
Output: Message M
Initialization: Read I_s
***Preprocessing of I_s*:**
Resize I_s to a square matrix of pixel values P_{ij}
Divide I_s into 8 × 8 blocks
Apply DCT in each block, P_{uv}
Generate an 8 × 8 quantization table, Q_t
Quantize each block by P_{uv}/Q_t and round them, Q_{uv}
Find DC values by $Q_{uv} \leftarrow Q_{uv}((u*8)-7, (v*8)-7)$ and binarize
***Extracting from LSB*:**
for each Q_{uv}
Extract the LSBs from Q_{uv} to find modified text, M_c
end for
Find cover image pixel values, C_{ij}
AES encrypted message, $M_{AES} = C_{ij} \oplus M_c$
Apply AES decryption on M_{AES} to get original message M

Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), correlation values, and histogram analysis are considered.

Table 1. Definitions of images used.

Image name	Grayscale/Color	Resolution	Format	Size
Lenna	Grayscale	512 × 512	BMP	257 KB
Cameraman	Grayscale	256 × 256	TIFF	63.7 KB
Baboon	Color	512 × 512	PNG	622 KB
Zelda	Grayscale	512 × 512	PNG	135 KB

5.1. Subjective Evaluation

The stego-image and the cover image should be indistinguishable visually. This can easily be measured by subtracting the pixel values of the stego image from cover image. **Figure 4** describes the result of subtraction of two images, which is a complete black image.

This experiment was also done with other images which are shown in **Figure 5**.

5.2. Objective Evaluation

Any algorithm that passes this evaluation should have a very good potentiality of not being detected by just only observing the image.

5.2.1. MSE and PSNR

MSE and PSNR are the two well-known objective image quality metrics to evaluate the standard and quality of any image. The MSE and PSNR are defined by using Equation (3) and (4) respectively.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(p_{ij} - q_{ij} \right)^2 \tag{3}$$

where, M = Height of the cover image,

N = Width of the cover image,

p_{ij} = Pixel value before embedding data,

q_{ij} = Pixel value after embedding data.

$$PSNR = 10 \times \log_{10} \frac{c_{\max}^2}{MSE} \tag{4}$$

where, $C_{\max}$ = Maximum pixel value which in case of our images is 255.

If the value of PSNR is between 30 - 40 decibels, then the quality of the stego-image is pretty good. A PSNR value above 40 decibels is considered as a very good stego-image and the changes are quite unnoticeable [22]. The better the PSNR value, the better the quality of the steganography. **Table 2** shows results of the experiment based on MSE & PSNR.

5.2.2. Correlation

Correlation is the statistical measurement of similarities between two images. Equation (5) calculates the correlation between two images.

(a) (b) (c)

Figure 4. (a) Lenna cover image; (b) Lenna stego-image; (c) Difference image.

(a) (b)

(c)

Figure 5. Cover vs stego-image of (a) Cameraman; (b) Baboon; (c) Zelda.

Table 2. MSE & PSNR values of different stego-images.

Image	MSE	PSNR in dB
Lenna	0.0334	62.89
Cameraman	0.0158	66.15
Baboon	0.0348	62.72
Zelda	0.0335	62.88

$$r = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(p_{ij}-\bar{p}\right)\times\left(q_{ij}-\bar{q}\right)}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(p_{ij}-\bar{p}\right)^{2}\right)\times\left(\sum_{j=1}^{M}\sum_{j=1}^{N}\left(q_{ij}-\bar{q}\right)^{2}\right)}} \quad (5)$$

From a range of 0 to 1, a stego-image having a correlation close to 0 represents no similarity with the cover image, nonetheless having the correlation value approaching 1 represents high identicality of the cover and the stego-image. Table 3 shows results of the experiment based on correlation values.

5.2.3. Histogram Analysis

Another important steganographic metric is to compare the histogram of the cover image and the stego-image. This comparison can reveal that an image has

Table 3. Correlation values of different stego-images and cover images.

Cover and Stego image	Correlation value
Lenna	0.9991
Cameraman	0.9995
Baboon	0.9988
Zelda	0.9987

Table 4. Comparison of proposed method with other methods based on PSNR values.

Method	Lenna	Baboon
Anurag *et al.*'s [23]	41.57 dB	41.62 dB
Chang *et al.*'s [24]	44.97 dB	44.68 dB
Hong *et al.*'s [25]	48.68 dB	48.66 dB
Lin *et al.*'s [26]	49.90 dB	49.92 dB
Singh *et al.*'s [27]	55.94 dB	55.92 dB
Maheswari *et al.*'s [28]	45.31 dB	45.53 dB
Proposed method	**62.89 dB**	**62.72 dB**

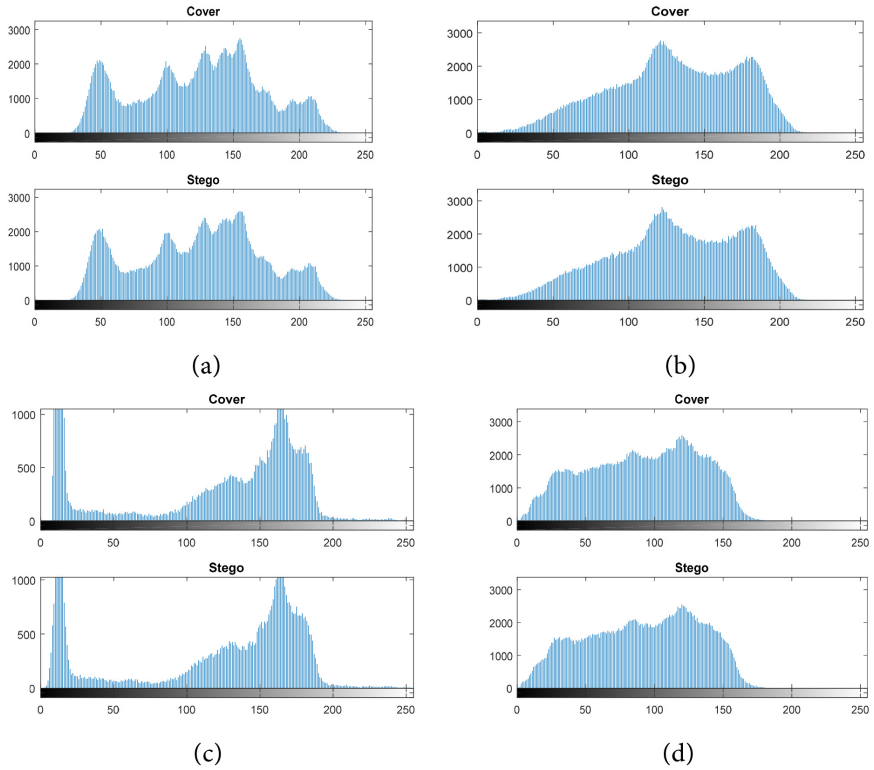

Figure 6. Cover vs stego-image histograms of (a) Lenna; (b) Baboon; (c) Cameraman; (d) Zelda.

embedded data if there is a noticeable difference in the histograms. **Figure 6** shows the histograms of cover and corresponding stego-image. The histograms

of the cover image and the stego-image are very close and the change is merely distinguishable. This enhances the performance of the proposed method.

These above mentioned parameters measure the quality of the stego-image and efficiency of the proposed embedding algorithm. From the results, it is found pretty good PSNR value and the correlation is also very good. Visually, the stego-image is almost equivalent to the cover image. So, the proposed algorithm can be said as an efficient algorithm for image steganography on different sizes and formats of images. A statistical comparison of PSNR values of different methods of image steganography and the proposed method is also shown in **Table 4**.

6. Conclusions

The proposed algorithm for embedding and extracting has two levels of security, it is a combination of both AES Cryptographic and DCT Steganographic methods which have proved to improve data security as well as the data secrecy. Using spatial domain to modify the images may cause suspicion to attackers due to its additive noise on the cover image. For the benefit of human comprehension, frequency domain is often used since it hides the data more efficiently and thus the distortion of the pixel data is less noticeable to the naked eyes. This is why we use DCT, or Discrete Cosine Transform, in the proposed algorithm.

To justify the proposed algorithm as efficient, the value of correlation needs to be very close to 1 and PSNR value must be more than 40 dB. We got a correlation value of 0.9991, which is really close to 1, calculating the correlation value of the Lenna image of 512 × 512 resolution. The PSNR value calculated to hide 512 bits of data in a 512 × 512 Lenna image was 62.89 dB. Higher Correlation and PSNR here mean that there is better invisibility of our data in the cover image. This shows that the proposed algorithm generated standard stego-images with excellent performance metrics.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Morkel, T., Eloff, J.H. and Olivier, M.S. (2005) An Overview of Image Steganography. *Information Security South Africa*, Johannesburg, 29 June-1 July 2005, 1-11.

[2] Wang, H. and Wang, S. (2004) Cyber Warfare: Steganography vs. Steganalysis. *Communications of the ACM*, **47**, 76-82. https://doi.org/10.1145/1022594.1022597

[3] Kour, J. and Verma, D. (2014) Steganography Techniques—A Review Paper. *International Journal of Emerging Research in Management & Technology*, **3**, 132-135.

[4] Ge, H., Huang, M. and Wang, Q. (2011) Steganography and Steganalysis Based on Digital Image. 4*th International Congress on Image and Signal Processing*, Shanghai, 15-17 October 2011, 252-255. https://doi.org/10.1109/CISP.2011.6099953

[5] Lie, W.N. and Chang, L.C. (1999) Data Hiding in Images with Adaptive Numbers of

Least Significant Bits Based on The Human Visual System. *Proceedings of IEEE International Conference on Image Processing*, Kobe, 24-28 October 1999, 286-290.

[6] Chan, C.K. and Cheng, L.M. (2004) Hiding Data in Images by Simple LSB Substitution. *Pattern Recognition*, **37**, 469-474. https://doi.org/10.1016/j.patcog.2003.08.007

[7] Ker, A.D. (2005) Steganalysis of LSB Matching in Grayscale Images. *IEEE Signal Process*, **12**, 441-444. https://doi.org/10.1109/LSP.2005.847889

[8] Wu, D.C. and Tsai, W.H. (2003) A Steganographic Method for Images by Pixel-Value Differencing. *Pattern Recognition Letters*, **24**, 1613-1626. https://doi.org/10.1016/S0167-8655(02)00402-6

[9] Zhang, X. and Wang, S. (2004) Vulnerability of Pixel-Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security. *Pattern Recognition Letters*, **25**, 331-339. https://doi.org/10.1016/j.patrec.2003.10.014

[10] Kawaguchi, E. and Eason, R.O. (1998) Principles and Applications of BPCS Steganography. *Proceedings of SPIE*: *Multimedia Systems and Applications*, Boston, 22 January 1999, Vol. 3528, 464-473. https://doi.org/10.1117/12.337436

[11] Maya, S.T., Miyatake, M.N. and Meana, H.P. (2006) An Image Steganography System Based on BPCS and IWT. 16*th International Conference on Electronics*, *Communications and Computers*, Puebla, 13 March 2006, 51. https://doi.org/10.1109/CONIELECOMP.2006.14

[12] Bansal, D. and Chhikara, R. (2014) An Improved DCT Based Steganography Technique. *International Journal of Computer Applications*, **102**, 46-49. https://doi.org/10.5120/17887-8861

[13] Jameelah, H.S. (2012) Discrete Cosine Transform Using in Hiding Image Technique. *Al-Mustansiriyah Journal of Science*, **23**, 157-168.

[14] Gunjal, M. and Jha, J. (2014) Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm. *International Journal of Computer Trends and Technology*, **11**, 144-150. https://doi.org/10.14445/22312803/IJCTT-V11P131

[15] Tseng, H.W. and Chang, C.C. (2004) Steganography Using JPEG Compressed Images. 4*th International Conference on Computer and Information Technology*, Wuhan, 14-16 September 2004, 12-17.

[16] Hashad, A.I., Madani, A.S. and Wahdan, A.E.M.A. (2005) A Robust Steganography Technique Using Discrete Cosine Transform Insertion. *International Conference on Information and Communication Technology*, Cairo, 5-6 December 2005, 255-264. https://doi.org/10.1109/ITICT.2005.1609628

[17] Seivi, G.K., Mariadhasan, L. and Shunmuganathan, K.L. (2012) Steganography Using Edge Adaptive Image. *International Conference on Computing*, *Electronics and Electrical Technologies*, Kumaracoil, 21-22 March 2012, 1023-1027.

[18] Banik, B.G. and Bandyopadhyay, S.K. (2015) Implementation of Image Steganography Algorithm Using Scrambled Image and Quantization Coefficient Modification in DCT. 2015 *IEEE International Conference on Research in Computational Intelligence and Communication Networks*, Kolkata, 20-22 November 2015, 400-405. https://doi.org/10.1109/ICRCICN.2015.7434272

[19] Daemen, J. and Rijmen, V. (2002) The Design of Rijndael. Springer-Verlag, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-04722-4

[20] Sheidaee, A. and Farzinvash, L. (2017) A Novel Image Steganography Method Based on DCT and LSB. 9*th International Conference on Information and Knowledge Technology*, Tehran, 18-19 October 2017, 116-123. https://doi.org/10.1109/IKT.2017.8258628

[21] Diniz, P.S.R., Silva, E.A.B.D. and Netto, S.L. (2010) Digital Signal Processing-System Analysis & Design. Second Edition, Cambridge University, Cambridge.

[22] Cheddad, A., Condell, J., Curran, K. and McKevitt, P. (2010) Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Process*, **90**, 727-752. https://doi.org/10.1016/j.sigpro.2009.08.010

[23] Anurag and Meena, S. (2018) Color Image Steganography Using Random Key Matrix. 3*rd International Conference for Convergence in Technology*, Pune, 6-8 April 2018, 1-5. https://doi.org/10.1109/I2CT.2018.8529425

[24] Chang, C.C., Chou, Y.C. and Kieu, T.D. (2008) An Information Hiding Scheme Using Sudoku. 3*rd International Conference on Innovative Computing*, *Information and Control*, Dalian, 18-20 June 2008, 17-21. https://doi.org/10.1109/ICICIC.2008.149

[25] Hong, W., Chen, T.S. and Shiu, C.W. (2008) A Minimal Euclidean Distance Searching Technique for Sudoku Steganography. *International Symposium on Information Science and Engineering*, Shanghai, 20-22 December 2008, 515-518.

[26] Lin, C.N., Chang, C.C., Lee, W.B. and Lin, J. (2009) A Novel Secure Data Hiding Scheme Using a Secret Reference Matrix. 5*th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Kyoto, 12-14 September 2009, 369-373. https://doi.org/10.1109/IIH-MSP.2009.143

[27] Singh, A. and Singh, H. (2015) An Improved LSB Based Image Steganography Technique for RGB Images. *IEEE International Conference on Electrical*, *Computer and Communication Technologies*, Coimbatore, 5-7 March 2015, 1-4. https://doi.org/10.1109/ICECCT.2015.7226122

[28] Maheswari, S.U. and Hemanth, D.J. (2014) Frequency Domain QR Code Based Image Steganography Using Fresnelet Transform. *International Journal of Electronics and Communications*, **69**, 539-544. https://doi.org/10.1016/j.aeue.2014.11.004