A Proposal to Improve the Bit Plane Steganography based on the Complexity Calculation Technique

Cho Do Xuan
Information Assurance Department
FPT University, Hanoi
Vietnam

***Abstract*—The video steganography technique is being studied and applied a lot today because of its benefits. In particular, the video steganography technique using Bit-Plane Complexity Segmentation (BPCS) has increasingly proven its effectiveness compared to other methods. In this paper, based on the theoretical basis of the BPCS method, we propose a new method to improve the efficiency of the steganography process. Accordingly, our improvement proposal in this paper is improving the complexity formula of the bit planes. Our new formula not only has improved the steganographic thresholds in the bit planes to find more planes hiding secret information, but also has ensured the amount of information hidden in the video and their safety. The experimental results in the paper have not only demonstrated the effectiveness of our proposed method but also provided a new mechanism for digital image analysis in general and video steganography techniques in particular.**

Keywords—Steganography; video steganography technique; bit-plane complexity segmentation (BPCS); complexity formula

I. Introduction

A. Introduction to BPCS Method

In the study [1], Kawaguchi et al. presented an image steganography method based on the BPCS technique. The characteristic of this method is the use of images or video frames as the message vessel. Accordingly, the image is divided into bit planes based on the depth value of the image. With each bit-plane, we can divide it into noise-like blocks or informative blocks, then replacing noise-like by the blocks of secret information that have similar noisy property will not change the image quality. The process of embedding information in video using BPCS technique includes the following steps [1]:

1) Determining the noise-like block. Fig. 1 illustrates an example of the noise-like block. To determine noise-like block, the study [1] proposed Black-White border method. Accordingly, in Black-white border, the complexity is determined by the length of the border of the Black-White regions in blocks horizontally and vertically. For example, a black pixel surrounded by 4 white pixels has a border length of 4. The longer the block has the border length, the higher the complexity. Based on the above definition, we have the following formula to determine the complexity of a block with size 2n * 2n [1]:

$$\alpha = \frac{k}{2*2n*(2n-1)} \qquad (1)$$

Where:

- α is the complexity of the block.
- k is the number of borders in contact between 2 regions.
- $2*2n*(2n-1)$ is the number of borders that are in contact maximum possible with the block. It is the number of borders in the chessboard.

2) Identifying complexity threshold: The process of identifying the complexity threshold to determine how much complexity is, the region is noise, and how much complexity is, the region is informative. To do that, the researchers tested on blocks of size 8 * 8. The use of blocks 8 * 8 is to match the complexity of the current method. For blocks 8 * 8, the average value of α is 0.5, the informative blocks have α in between 0 and 0.5 and only accounted for 6.67×10^{-14}%. From these values, one normally choose a complexity threshold as α_0 = 0.3 for block 8 * 8 [1].

3) The conjugation property. This property ensures the safety of the information that needs to be hidden in the noise-like regions. Accordingly, when information is divided into appropriate blocks and is calculated complexity, if it is an informative block, it will be conjugated to be a block with higher noise for embedding information. The conjugation property is stated as [1]: With a block P with complexity α, there exists only a block conjugate of P denoted P* has complexity is α' = 1 - α. This block is an XOR result between P and the block W_c (alternating black and white blocks starting with white pixel).

4) Canonical gray coding: This is the process of processing images to embed information. Accordingly, suppose that b_i *and* g_i are respectively the i-th bit of the PBC and CGC codes with n-bits of data we have [2].

$b_0 b_1 \dots b_{n-1}$ *and* $g_0 g_1 \dots g_{n-1}$

The formula for switching between two coding systems is:

$$g_i = \begin{cases} b_0 \ ; \text{Where } i = 0 \\ b_{i-1}\ xor\ b_i \text{ Where } i > 0 \end{cases} \qquad (2)$$

$$b_i = \begin{cases} g_0 \text{ Where } i = 0 \\ b_{i-1}\ xor\ b_{i-1} = g_0\ xor \dots xor\ g_i \text{ Where } i > 0 \end{cases}$$

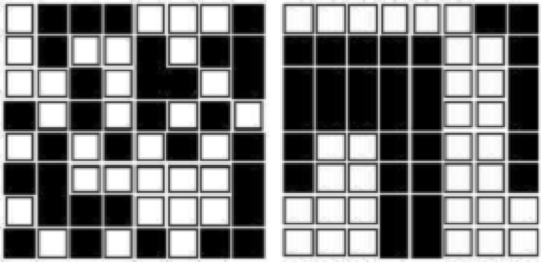


Fig. 1. Examples of Bit Planes for Determining the Noise-like Block.

B. The Problem of Improving the BPCS Method

Based on the process of processing and embedding information, it can be seen that improving the BPCS method is based on two main methods [2, 3, 4, 5]:

- Improvement in the pre-processing process. This is an improved method to be performed at the pre-processing step. The characteristic of this method is the modification of the input data (namely the image used for embedding) in order to make embedding more efficient. Some of the approaches are: Use of Gray coding; handling the vessel to increases the image sharpness; randomizing input data.
- Improving the embedded algorithm. The approaches usually focus on two main improvement methods: i) Improvement of complexity threshold. This approach mainly refers to 2 improvement methods: the complexity threshold for each bit plane and the Dynamic Threshold; ii) Improvement of the formula. There are 2 formulas currently used as Run-Length Irregularity and Border Noisiness.

C. Contributions of the Paper

Our research is presented as follows: the urgency of the research problem is presented in Section I. In Section II, we present the process of researching, surveying, and evaluating related works. In Section III, we present our surveys and reviews of problems of proposing improvements for BPCS. This review and survey help us have a basis to propose our new method in the paper. Finally, in Section IV, we present the experimental method to evaluate and compare the effectiveness of our proposed method with other methods. The practical significance and scientificity of our paper include:

- Proposing improvements for video steganography techniques based on the approach about the calculation formula. Accordingly, we propose a new calculation formula to evaluate the complexity of the frames. Details of the proposed algorithm and its feasibility assessment are described in section III.C of the paper.
- We conduct experiments, evaluate, and compare to see the effectiveness of our approach with other research directions. The experimental results in section IV.B.2 proved the correctness of our method. At the same time, the research results in the paper also provide a new approach to calculating the complexity of the image in order to serve for the analysis of digital images in general and hiding information by the BPCS method in particular.

II. Related Works

A. BPCS Technique and Some Improvements

The study [5] proposed the Modified BPCS technique by combining hybrid cryptography algorithms between RSA and DES to create noise for secret messages. Piyush and Paresh [6] proposed a combined method of cryptography, steganography, and multimedia data hiding. In this method, the authors used a reference database to provide higher security levels. First, the authors used the DES algorithm to encrypt the message, then using a modified bit encoding technique to save the cipher in the image. For each byte of data, one cover pixel will be edited. The study [7] combined the AES cryptography algorithm and the BPCS steganography algorithm to hide a large amount of data in image. In the study [8], the authors proposed applying the BPCS method and FPGA model to ensure information security for secret information. In the study [9], the authors proposed combining the BPCS method with the Huffman cryptography algorithm to improve the quality of hiding information.

In the study [10], the authors proposed a method of combining BPCS with fuzzy logic techniques. This study applied the principles of fuzzy sets to classify the bit-plane into three sets: informative, partly informative, and noise region. This is expected to classify the bit-plane in a more objective approach. Finally, the Mamdani fuzzy inference is used to make decisions on which bit-plane will be replaced with a message based on the classification of bit-plane and the size of the message that will be inserted. This helps improves the message capacity of the images. The research could improve BPCS steganography techniques to insert a message in a bit-pane with more precision. Thus, the container image quality would be better. Seeing that the PSNR value of the original image and the stego-image is only slightly different. In addition, the studies [11, 12, 13, 16] listed some video steganography methods, difficulties, challenges as well as the advantages and disadvantages of video steganography techniques. Besides, Spaulding et al. [14] presented the BPCS steganography method with the embedded zerotree wavelet (EZW) lossy compression. This method used the DWT coefficients to represent pixels of the original frame. Therefore, the BPCS steganography can be applied to DWT coefficient sub-bands containing different features. Similarly, Noda et al. [15] proposed a video steganography technique using the BPCS and wavelet compressed video.

On the other hand, Sharma et al. [17] presented a number of research and evaluation results of the effectiveness and safety of BPCS and LSB techniques. The research results showed that in the BPCS technique, all the data was embedded in a complex noisy blue plane. The embedding capacity of BPCS techniques and LSB techniques is high. On comparison, it is found that the LSB steganography and LSB using the secret key perform the best on the basis of PSNR. According to the entropy and correlation point of view, the best results are shown by the status bit and BPCS steganography techniques.

B. Some Studies of Combining Encryption with Steganography

In the study [18], Shifa et al. proposed a method of combining the AES encryption with LSB steganography technology in order to distribute and exchange keys. The experimental results show that the LSB model combined with AES encryption has a good effect on the speed and impact degree on the message vessel. In the study [19], Dhall proposed the first method of using Quantum Cryptography to increase the security of the application. Saha [20] et al. published a steganography method based on Exploiting Modification Direction using the hashed-weightage Array. Kait [21] applied the BPCS technique as a technique to noise information in order to ensure data security using FPGA implementation. In addition, the studies [22-26] proposed to apply some common steganography techniques such as Discrete Cosine Transform (DCT), LSB, Least Significant bit Matched Revisited (LSBMR), DWT to protect data in communication applications.

III. Evaluating and Recommending Improvements of BPCS

A. Improvement on Complexity Threshold

With basic BPCS, we usually choose only one complexity threshold for the whole bit-plane. The study [3] proposed a method to apply the complexity threshold for each bit plane. Accordingly, the authors demonstrated that the complexity threshold from the low bit plane will gradually decrease to zero. Usually, at the highest bit planes, no change will be made here because changing the bit here will strongly affect image quality. On the contrary, the lower bit planes have a higher threshold to increase the ability to embed information.

The study [3] proposed improvement direction for the BPCS algorithm based on Dynamic Threshold. This method makes some adjustments to the threshold setting. These threshold values have no default values. They can be adjusted manually according to the actual conditions. This algorithm can avoid the analyzer from detecting the existence of secret information using complex statistical analysis of the entire graph, thus further enhancing the security of steganography. The basis of the Dynamic Threshold improvement method is based on the Chaos theory. Accordingly, the Chaos theory is a type of behavior controlling nonlinear dynamical rule. In this research, the authors used the logistic mapping method to create chaos series according to the formula:

ak+1 = μ* ak*(1 - ak), k= 0,1,2. (3)

The moving value is in the range [0, 1] and μ is a control parameter or a split parameter. When 3.5699456... <μ <= 4, logistic maps operate in a chaotic state [3]. The generated data stream is disordered and it is similar to random noise. Processing the obtained chaos series, mapped to {0, 1} and {-2, -1, 0, 1, 2}.

B. Improving the Formula Determining the Complexity

To assess whether the blocks are complex or not, the studies are based on the complexity of the black-and-white border region. However, it is not always the best approach. For example, blocks with periodic patterns like the chessboard will be recognized for complexity in this way as shown in Fig. 2 α_a = 1 and α_b = 1/2.

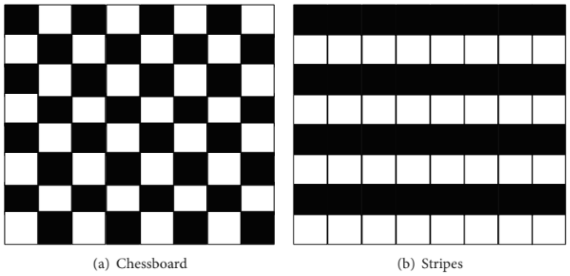

(a) Chessboard (b) Stripes

Fig. 2. Example of Blocks with Large α but those are not Complicated.

1) Determining the noise-like block: The Run-Length Irregularity is the histogram of the lengths of both black and white pixels in a row or a column [2]. Assume that:

- h [i] is the frequency of runs of i pixels either in black or in white.
- n is the length of the sequence of pixels.
- h_s to measure the irregularity of a binary pixel sequence.

$$P_i = \frac{h[i]}{\sum_{j=1}^{n} h[j]} \quad (4)$$

The value $h_s \in [0; 1]$ and denoted by:

$$h_s = \sum_{i=1}^{n} h[i] log_i p_i \quad (5)$$

If the size of the block is $n \times n$ and r_i and c_j are respectively the i-th row and j-th column of a block, then the run-length irregularity β of a block is defined with $\bar{X}$ which is the mean of all the elements of X.

$$\beta = min\{\widehat{H_s(r)}, \widehat{H_s(c)}\}$$

$$\widehat{H_s(r)} = \{\widehat{h_s}(r_0), \dots\dots, \widehat{h_s}(r_{n-1})\}$$

$$\widehat{H_s(c)} = \{\widehat{h_s}(c_0), \dots\dots, \widehat{h_s}(c_{n-1})\}$$

If according to the definition, the smaller row and column averages are taken as the value of the run-length irregularity β. As shown in Fig. 3, they are both periodic in row or column. The result is that every run-length irregularity β is 0, so they are simple and cannot be used for embedding information. The run-length irregularity β is only useful in rows or columns. If the block is frequently in other directions, there will be nothing to do with it.

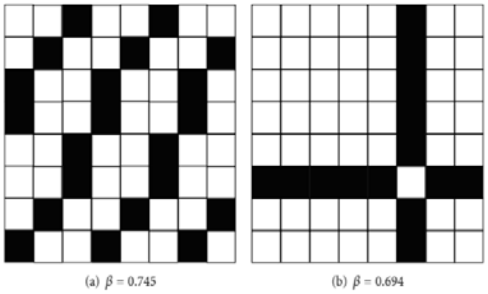

(a) $\beta = 0.745$ (b) $\beta = 0.694$

Fig. 3. Examples of Blocks with Large β but those are not Complicated.

2) Border noisiness: If the data is embedded on the boundary of the noise region and the informative region of the block in the image, then the noisy regions would grow. As a result, the image will be evidently changed. Border Noisiness is based on the difference between adjacent binary pixel sequences in a block. In a similar way, if the block size is *n x n* and r_i and c_j are respectively the i-th row and j-th column of a block, then the *Border Noisiness* γ of a block is defined as follows [2]:

$$\gamma = \frac{1}{n}\min\{E_f[P_x(r), E_f[P_x(c)]\} \qquad (6)$$

Where $\rho(x)$ is the number in the binary string X and

$$P_x(r) = \{\rho(r_0 \oplus r_1), \dots., \rho(r_{n-2} \oplus r_{n-1})\}$$

$$P_x(c) = \{\rho(c_0 \oplus c_1), \dots., \rho(c_{n-2} \oplus c_{n-1})\}$$

$$E_f(X) = \frac{1 - V(X)}{max_X\{V(X)\}} .\bar{X}$$

Where: $X = \{x_0, \dots., x_{m-1}\}$, $V(X)$ is the variance of X, and $\bar{X}$ is the mean of X.

Border Noisiness is used to check if many black and white pixels are well distributed over a block along with both horizontally and vertically. Although blocks in Fig. 3(a) and 3(b) both have large run-length irregularity β (a = 0.745, b = 0.694), their Border Noisiness are 0.294 and 0.048 respectively. Therefore, they are not complicated according to Border Noisiness and are not suitable for embedding data.

C. Our Proposal

We noticed that there is no exact formula or judgment about the definition of complexity for an information block. The black-white border is just one of many formulas to determine this complexity. This formula is simple, useful, and gives the best results. But it still has some shortcomings. Therefore, we propose a novel method to calculate complexity. This method is quite similar to the Black-white border but it exploits another aspect that is the number of black and white regions in the block (the Black-white border uses the number of black and white borders). This formula is based on the assumption that the higher the number of black-and-white regions a block has, the higher the complexity of the block is and vice versa. From the above assumption, we propose the formula for calculating the complexity for a block of size 2n * 2n as follows:

$$\partial = \frac{k}{2n*2n} \qquad (7)$$

Where: *k* is the number of black and white regions in the block; *2n * 2n* is the maximum number of black and white regions that a block of size *2n * 2n* can receive. To verify this assumption and to show the better aspects of this formula than the previous formulas, we will conduct a comparison with some blocks (see Fig. 4 and Fig. 5, 6).

From Fig. 4(a) we calculate the following values: α = 0.42; β = 0.198; ∂ = 0.04.

Fig. 4(b) gives the following values: α = 0.42; β = 0.123; ∂ = 0.156.

Fig. 4(c) gives the following values: α = 0.58; β = 0.745; ∂ = 0.14.

Fig. 4(d) gives the following values: α = 0.285; β = 0.694; ∂ = 0.14.

With the naked eye, we can see which are informative blocks with clearly divided black and white regions. However, with the original formula, these images give high results, in contrast to the Border Noisiness formula and the formula that we proposed. Fig. 5 below is an example that shows a weak point of Border Noisiness. On the other hand, the proposed way still indicates that these are informative blocks.

From Fig. 5(a), we calculate the following values: $\alpha = 1$; $\beta = 0$; $\partial = 1$.

Fig. 5(b) gives the following values: $\alpha = 1$; $\beta = 0$; $\partial = 0.07$.

Can be seen that: Although giving good results with the previous blocks, but up to the chessboard block, the proposed method still gives high results. But for stripe block, it still gives low results in contrast to the Black-white border. Through the above examples, we can see that our proposed method gives better results than the original algorithm. Next, to evaluate the feasibility of the complexity formula, we will conduct the experiment of embedding information using the BPCS method and evaluate the embedded results based on measures.

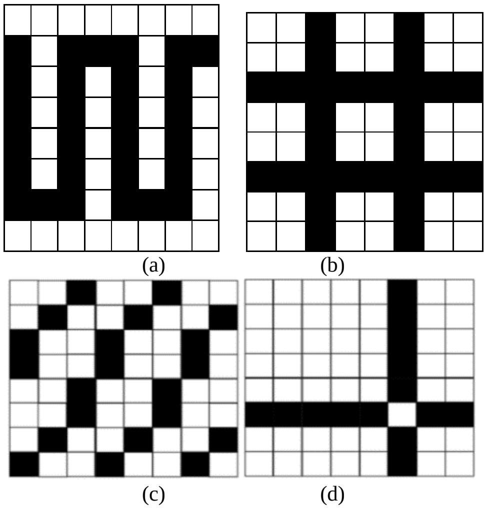

(a) (b)
(c) (d)

Fig. 4. Examples of Noise Blocks.

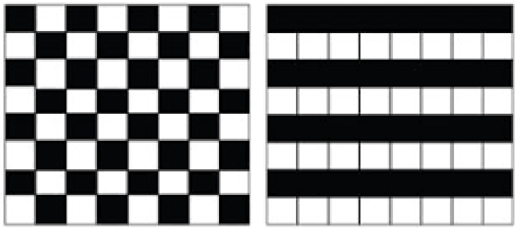

(a) (b)

Fig. 5. Example of Informative Blocks showing the Weakness of Border Noisiness.

IV. Experiments and Evaluation

A. Evaluation Criteria

To conduct experiments and evaluations, we use a number of criteria to evaluate as follows.

1) Peak signal-to-noise ratio: The Peak signal-to-noise ratio (PSNR) is a measure of the difference between the original image and the stego image. Comparing the results of two algorithms should be based on the same codecs and the same data content. The simplest way is defining through the mean squared error (MSE) used for 2-dimensional images with size m × n where I and K are the original image and the stego image [4].

$$MSE = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(C_{ij} - R_{ij})^2 \qquad (8)$$

PSNR is defined by [4]:

$$PSNR = 10\log_{10}\frac{(2^b - 1)^2}{MSE} \qquad (9)$$

2) Embedding capacity: Embedding capacity is the maximum amount of data that an image can be successfully embedded by a steganography algorithm. This criterion depends on the input image data and the number of embedded bits [4].

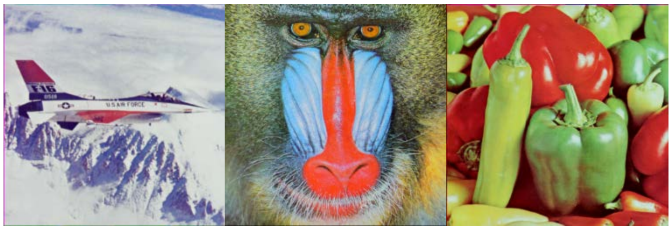
$$bpp = \frac{hidden\ bits}{total\ bits} \qquad (10)$$

B. Experiment And Evaluating Formula Improvement Methods

1) Scenario and experimental data: To evaluate the effectiveness of our proposed formula, we will do experiments on some images with a resolution of 512 * 512, which is the resolution commonly used for hiding information. Fig. 6 below presents the images used to hide information.

2) Experimental results: Table I below shows the distribution of thresholds. From there, we select a complexity threshold that balances image quality and memory capacity.

Through the statistics in Table I and Fig. 7, we can see that with the proposed formula, blocks 8 * 8 usually have a value in the range from 0 to 0.2. This proves that the majority of blocks have threshold values from 0 to 0.2. The distribution diagram is similar to that of the classic formula. The only difference is that the equilibrium threshold is 0.2 and the threshold of the classic formula is 0.5. With classic formula, the threshold will be selected from 0.3 to 0.5 so we can speculate that the threshold of the improved formula is from 0.12 to 0.2. With this range, we can also see the ability to hide is about 50%. With the selected complexity threshold of 0.14, the experimental process will proceed as follows. Specifically, to test the maximum ability to hide information, we will use 3 images in Fig. 6 as vessels, and then we check the maximum ability to hide information on each photo to give the results of the ability to embed. Besides, to test PSNR, we will embed the Beagle.png image (Fig. 8) to produce the results and calculate PSNR between the original image and stego image.



(a) Jet.png (b) Baboon.png (c) Peppers.png

Fig. 6. Three Experimental Images.

TABLE I. Threshold Distribution of the Images in Figure 6

Capacity	Baboon.png	Peppers.png	Jet.png
0.05	92.85%	64.59%	60.56%
0.1	80.74%	52.48%	48.44%
0.15	56.52%	44.41%	40.37%
0.2	40.37%	24.22%	12.11%
0.25	20.18%	0.08%	0.08%
0.3	0.04%	0.00%	0.00%

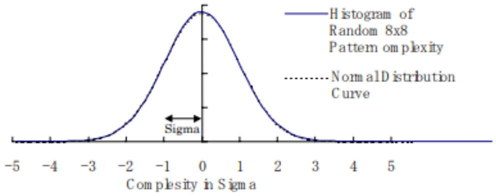


Fig. 7. Distribution Diagram of the Thresholds Calculated by the Classical Formula [1].

Fig. 8. Beagle.png

3) Experimental results: From the results in Tables II and III, it can be seen that the ability to hide information of improved BPCS, which we propose, is much better than classic BPCS with a complexity threshold of 0.4. The ability to hide information will increase by about 10% to 15% of the image capacity. Although this ability increases significantly, when compared to the PSNR index, it is not much different from the original algorithm. Although the PSNR index decreases by about 0.01, increasing the ability to hide information brings great benefits. This can be seen as a valuable improvement. Here we can increase the complexity threshold to 0.15 or 0.145 in exchange for a higher PSNR depending on the intended use.

TABLE II. COMPARING THE ABILITY TO HIDE INFORMATION OF EACH METHOD

Capcity	**BPCS [1] $\alpha = 0.4$**	**BPCS [our proposal] $\partial = 0.14$**
Baboon.png	3503297 bit = 55.68 %	**3810240 bit = 60.56 %**
Peppers.png	2612544 bit = 41.52 %	**3048192 bit = 48.45 %**
Jet.png	1821056 bit = 28.94 %	**2540160 bit = 40.37 %**

TABLE III. COMPARING IMAGE QUALITY AFTER HIDING INFORMATION

Capcity	**BPCS [1] $\alpha = 0.4$**	**BPCS [our proposal] $\partial = 0.14$**
Baboon.png	53.43	**53.42**
Peppers.png	53.44	**53.43**
Jet.png	53.44	**53.43**

V. CONCLUSION

Applying the BPCS steganography technique to hide secret information or protect vessels is one of the best current approaches. In this paper, based on the procedure and the mathematical basis of the BPCS steganography technique, we proposed an innovative method to improve the quality of hiding information. The experimental results, which we performed in Tables II and III, proven that the method of improving the complexity calculation algorithm in bit planes gave good results not only for the ability to hide information but also to ensure the image quality. The research results will allow having many criteria to select the bit planes based on calculating their complexity for hiding information. At the same time, our computation proposal will also provide a new way for problems related to analyzing digital images in the face of the diversity and rapid development of the multimedia field. In the future, we will apply many other improved methods, especially the applying of different thresholds for each plane bits, in order to increase the capacity to hide information as well as image quality when hiding.

REFERENCES

[1] Eiji Kawaguchi, Richard O. Eason, “Principles and applications of BPCS steganography,” Multimedia Systems and Application, vol. 35(2), pp. 464-473, 1999.

[2] Peipei Shi, Zhaohui Li, “An improved BPCS steganography based on dynamic threshold,” Proceedings of International Conference on Multimedia Information Networking and Security, Nanjing, Jiangsu, China, pp. 387-391, 2010.

[3] Shuliang Sun, “A New Information Hiding Method Based on Improved BPCS Steganography,” Advances in Multimedia, 2015.

[4] Vipul J Patel, Ms. Neha Ripal Soni, “Uncompressed Image Steganography using BPCS: Survey and Analysis,” OSR Journal of Computer Engineering, vol. 15, pp. 57-64, 2013.

[5] Smita P. Bansod, Vanita M. Mane, R. Ragha, “Modified BPCS steganography using Hybrid cryptography for improving data embedding capacity,” Proceedings of International Conference on Communication, Information & Computing Technology (ICCICT). Mumbai, India, pp. 1-6, 2012.

[6] P. Marwaha, “Visual cryptographic steganography in images,” Proceedings of Computing Communication and Networking Technologies (ICCCNT). Karur, India, pp. 1-6, 2010.

[7] M. Goljan, J. Fridrich, R. Du, “Distortion-free data embedding,” Proceedings of 4th Information Hiding Workshop, pp. 27-41, 2001.

[8] Vikas S. Kait, Bina Chauhan, “BPCS steganography for data security using FPGA implementation,” Proceedings of 2015 International Conference on Communications and Signal Processing (ICCSP). Melmaruvathur, India, pp. 1887-1891, 2015.

[9] Tayal, N., Bansal, R., Dhal, S. et al, “A novel hybrid security mechanism for data communication networks,” Multimed Tools Appl, vol. 76, pp. 24063–24090, 2017.

[10] Rahmad Hidayat, “Klasifikasi Bit-Plane Noise untuk Penyisipan Pesan pada Teknik Steganography BPCS Menggunakan Fuzzy Inference Sistem Mamdani,” Jurnal Rekayasa Elektrika, vol 11, pp. 101- 108, 2015.

[11] Ramadhan J. Mstafa, Khaled M. Elleithy, Eman Abdelfattah, “Video steganography techniques: Taxonomy, challenges, and future directions,” Proceedings of 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT). Farmingdale, NY, USA, pp. 1-6, 2017.

[12] Mstafa R.J., Elleithy K.M., “Compressed and raw video steganography techniques: a comprehensive survey and analysis,” Multimed Tools Appl, vol. 76, pp. 21749–21786, 2017.

[13] Gerrit Cornelis LANGELAAR, “Real-time Watermarking Techniques for Compressed Video Data,” Veenendaal, ISBN 90-9013190-6, 2000.

[14] Spaulding J, Noda H, Shirazi MN, Kawaguchi E, “BPCS steganography using EZW lossy compressed images,” Pattern Recogn Lett, vol. 23, pp. 1579–1587, 2002.

[15] Noda H, Furuta T, Niimi M Kawaguchi E, “Application of BPCS steganography to wavelet compressed video,” Proceedings of 2004 International Conference on Image Processing ICIP’04. Singapore, pp. 2147–2150, 2004.

[16] Y Liu, S Liu, Y Wang, H Zhao, S Liu, “Video steganography: A review,” Neurocomputing, vol. 335(28), pp. 238-250, 2019.

[17] Sharma, Rinku Ganotra, Reema Dhall, Sangeeta Gupta, Shailender, “Performance Comparison of Steganography Techniques,” International Journal of Computer Network and Information Security, vol. 10, pp. 37-46, 2018.

[18] S.A. Afgan et al. “Joint Crypto-Stego Scheme for Enhanced Image Protection with Nearest-Centroid Clustering,” IEEE Access, vol. 6, pp. 16189-16206, 2018.

[19] S. Dhall, R. Sharma, S. Gupta, “A multi-level steganography mechanism using quantum chaos encryption,” Multimed Tools Appl, vol. 79, pp. 1987–2012, 2020.

[20] Saha, S., et al. “Extended exploiting modification direction based steganography using hashed-weightage Array,” Multimed Tools Appl, vol. 79, pp. 20973–20993, 2020.

[21] V. S. Kait, B. Chauhan, “BPCS steganography for data security using FPGA implementation,” Proceedings of 2015 International Conference on Communications and Signal Processing (ICCSP). Melmaruvathur, pp. 1887-1891, 2015.

[22] G. L. Smitha, E. Baburaj, “A survey on image steganography based on Least Significant bit Matched Revisited (LSBMR) algorithm,” Proceedings of 2016 International Conference on Emerging Technological Trends (ICETT). Kollam, pp. 1-6, 2016.

[23] A. Y. AlKhamese, W. R. Shabana, I. M. Hanafy, “Data Security in Cloud Computing Using Steganography: A Review,” Proceedings of 2019 International Conference on Innovative Trends in Computer Engineering (ITCE). Aswan, Egypt, pp. 549-558, 2019.

[24] G. Maji, S. Mandal, N. C. Debnath, S. Sen., “Pixel Value Difference Based Image Steganography with One Time Pad Encryption,” Proceedings of 2019 IEEE 17th International Conference on Industrial Informatics (INDIN). Helsinki, Finland, pp. 1358-1363, 2019.

[25] S. Timarchi, M. A. Alaei, H. Koushkbaghi, “Novel algorithm and architectures for high-speed low-power ConText-based steganography,” Proceedings of 19th International Symposium on Computer Architecture and Digital Systems (CADS). Kish Island, pp. 1-6, 2017.

[26] G. Maji, S. Mandal, S. Sen, N. C. Debnath, “Dual image based LSB steganography,” Proceedings of 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom). Ho Chi Minh City, Viet Nam, pp. 61-66, 2018.