ISSN 2347 - 3983
Volume 9. No.10, October 2021
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter019102021.pdf
https://doi.org/10.30534/ijeter/2021/019102021

Multiple Image Based Dual Steganography Using Arnold Transform and Block Code Encoding

R.Roshini [1], Dr.C.Meena[2]
[1]Research Scholar, Avinashilingam Institute for Home Science and Higher Education for Women, India
roshini2910@gmail.com
[2]Head, Computer Centre, Avinashilingam Institute for Home Science and Higher Education for Women, India
cccmeena@gmail.com

Received Date : September 02, 2021 Accepted Date : September 25, 2021 Published Date : October 07, 2021

ABSTRACT

Security plays a crucial role in the field of Social media network. Securing the data become one among the largest challenges in the present scenario. Whenever we expect concerning the cyber security, the primary issue that involves our mind is ‘cyber crimes’ that are increasing vastly day by day. Embedding secret message into the image (Steganography) is associated with art and science of secure data communication wherever the key information or confidential information is hidden in host file. It's employed incompletely different helpful applications like secure electronic communication, health care and military. Confidential information’s are unremarkably keep in digital media and transmitted via network cause of rapid growth of internet. In this paper, steganography techniques which might be used to safeguard the information from intruders. Here, Steganographic technique is used to hide multiple secret images into a single 24-bit cover image using Least Significant Bit (LSB) and dual steganography method. Multiple secret images are scrambled and encoded before hiding into cover image using Arnold Transform and Block Code Encoding. The Proposed technique is Block Code Encoding to convert Secret message to binary and bit pairs to form safer information. The main goals of proposed work offers security and high limit based steganography plan of concealing a massive size secret image into a bit size cover image, to enhance security using dual steganography, image quality and to reduce error.

Key words: Arnold Transform, Block Code Encoding, LSB, Security, Steganography.

1. INTRODUCTION

In modern digital world, Information security is essential in network communication. One of the technique for securing information called Steganography. Steganography tries to hide the mere existence of any secret message by embedding it in some rather innocent looking cover media (image, video, audio etc.) whereas cryptography scrambles the secret message into some gibberish that can only be unscrambled with the help of some key or algorithm. The primary difference is that in cryptography a third party or an attacker knows that some secret is conveyed and can use its full energy to break the code and one day nobody else but the party is aware that it is transmitting the secret message. (i.e. it tries to find or force the key to breaking the secret) [1].

1.1 Characteristics of Steganography

Hiding Capacity: This feature deals with the scaleof data that may be hidden within the cover file. A bigger concealing capability permits use of a small cover and so reduces the band-width needed to transmit the stego–media [2].

Perceptual Transparency: Perceptual transparency is a very important feature of steganography. Every cover-media has certain information concealing capability. If a lot of information or information is hidden within the cover, then it leads to degradation of the cover–media [3].

Robustness: Robustness is that the ability of the hidden message to stay unbroken although the stego–media undergoes transformation, sharpening, linear and non-linear filtering, scaling and blurring, cropping and numerous different techniques [3].

Tamper–resistance: Of all the options, this feature is extremely necessary. This can be as a result of, if the offender is eminent in destroying the steganographic technique then the tamper–resistance property makes it tough for the offender or pirates to change or injury the initial information [17].

Undetectability: There should be no visual distinction between cover and stego object i.e. embedded message shouldn't be visible to human eye.

Security: An embedding algorithmic ruleis meant to be secure if the put ininformation could not be eliminated once location by the attacker. It depends upon the knowledge concerning the put in algorithmic rule and secret key.

1.2 Process of Image Steganography

Steganography is that the embedding of secret message in standard communication medium. It never brings doubt up in an exceedingly passive spectator. Digital images have high capability, redundancy and predominance. A large variety of photos are being transferred consistently within the web-based media. Image pixels are exceptionally corresponded and consequently additional information is place away while not selecting the visual nature of the image [2]. A steganography framework contains 2 primary advances shown in figure1, one for embedding and one for extraction. The embedding algorithm is concerned with inserting the message at intervals a carrier medium like image, audio or video, wherever the extraction method retrieves the embedded message from the cover. The extraction rule is less complicated than the embedding algorithm. One among the ways to enhance steganography security is to use the stego key which is needed to start out the embedding or extraction method. It’s used to create the extraction method computationally impossible for unauthorized users.

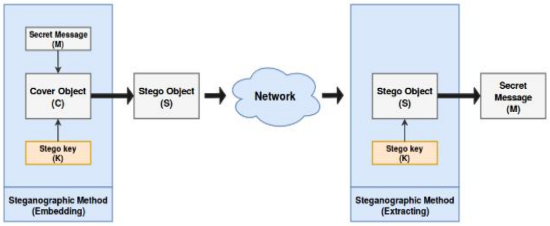

Figure 1:. Process of Image Steganography

The steganography terminology is listed below [3]:

• **Cover object (C):** The cover object represents the carrier medium used to hide the secret message (m). Varied kinds of object with redundancy in their representation is used as a cover object, like text, image, audio and video. It should be undistinguishable from the cover object.

• **Stego object (S):** The stego object refers to the modified cover object when concealing the key message. The cover and stego images should have a high degree of similarity to avoid a 3rd party suspecting the existence of the key message.

• **Message (M):** This refers to the information that must be hidden at intervals the cover object while not raising suspicion. Secret information is any digital information drawn in an exceedingly binary type.

• **Key (K):** The stego secret's an optional part used to management the embedding method. The extraction method is hardly possible without using the stego key. It is generated employing a pseudo-random variety generator (PRNG) [13].

• **Embedding method (Em):**the method of generating a stego object by concealment secret information within the cover object.

• **Extraction method (Ex):**The method of retrieving secret information from the stego object.

2. RELATED WORK

This chapter reviews some existing work that related to image security using steganography techniques.

Dai Hongzhu Cheng, JieLi and Yafeng (2020) [6] in this paper, authors planned steganographic rule that is predicated on division table modification and image scrambling within the DCT domain. First, the rule homogenizes the energy by scrambling the cover image to enhance the quantity of DCT coefficients appropriate for data embedding. Second, the embedding capability of the DCT block is set by the worth of the quantization table within the rule, different quantization tables get different embedding effects. Additionally, this paper proposes associate degree optimized modified quantization table. In depth experiments show that the planned rule achieves an excellent potential for confidential knowledge and undetectable image quality. This paper planned an appropriate quantization table to attain the optimum ratio of PSNR and embedding capability. This reference paper produced good image quality and embedding capability comparison with existing work.

Shanthakumari, R. and S. Malliga (2020) [7] in this approach, authors proposed the Elliptic Curve Cryptography rule is employed to encrypt the hidden data and also the encrypted knowledge inserted into a cover object by the method of the LSB Inversion rule. This mix of technology has with success reached the benchmark level of some essential properties referred to acknowledge confidentiality, integrity verification, capability and robustness that are the evidence to prove the excellent performance and effective implementation of this steganography method. This approach intensely tested through many steganalys is attacks like analysis of visual, histogram, and chi-square. The end result of the experimental result shown that the stego image has delivered the robust opposition force against all attacks. The information embedding capability has earned at an improved level compared with typical ways. From the outcomes it's seen that the planned arrange works higher once contrasted with this frameworks and high implanting limit is accomplished.

Liu, Hsing-Han & Lee and Chuan-Min (2019) [5] in this paper, authors used pixel value ordering (PVO) technique to enhance the steganographic capability. This work is based on pixel value calculation from 3 continuous and neighbor pixels are used for sequencing. The pixels with additional steganographic difference values in rows or columns are determined, when that the steganography and ciphertext retrieval steps are performed within the rows or columns of the digital image. This experiment results proven that the tactic replaces the block structure in frame choice by teams of continuously read pixels, i.e., each3components kind a pixel clusterwherever2 bits of confidential information is hidden, therefore up the steganographic capability effectively. An adjustment was created for calculation supported thought of each 3 component values mutually cluster, when that the steganographic capability of the digital image was maximized through scanning in rows and columns. Authors planned PVO activity theme through an experiment evaluated to assess whether or not its rule will increase the activity capability whereas maintaining the appropriate image quality. This work compared the results of the planned PVO theme to those of typical PVO activity ways to verify its efficiency. This proposed work tried to extend embedding capability with stable image quality as compared with existing work.

Fouad et al., (2019) [8] in this paper, a comparison of 2totally different techniques is proposed. The primary technique used Least significant Bit (LSB) with no encryption and no compression. Within the second technique, the key message is encrypted 1st then LSB technique is applied. Discrete cosine transform (DCT) is employed to rework the image into the frequency domain. The LSB rule is enforced in spatial domain during which the payload bits area unit inserted into the smallest amount important bits of cover image to develop the stego-image whereas DCT rule is enforced in frequency domain during which the stego-image is reworked from spatial domain to the frequency domain and also the payload bits are inserted into the frequency parts of the cover image. In this work, the performance of those2 techniques is evaluated on the basis of the parameters MSE and PSNR. Authors used LSB and DCT to scale back the range of bits/bytes during a file thus it is transmitted faster over slower net connections.

Maji et al., (2018) [9] in this paper, steganographic model utilizing dual image is proposed to expand the shortage of definition of the key even as to form it safer. It utilizes 2distinctivepicturesabove all reference image and cover image alongside a secret implant key (stego key). Reference image is isolated into blocks with allotted block-codes. Complete range of blocks and alternative embedding boundaries (block navigating heading, starting block and then forth) are place away within the implant key. Secret message modified over to double and bit sets are created. Spot sets of secret messages are encoded utilizing numerous blocks of reference image and refreshing a couple of LSB bits within the reference image. As an optional capability improvement module for text secret message word ordering primarily based encoding is applied. Eventually encoded bit stream is put in into the cover image utilizing any normal LSB technique with its own edges and faults. This work focused on enhancing high security by using LSB technique within the image blocks.

Sadik Ali Al-Taweel et al., (2018)[10] In this paper, authors proposed Arnold Transform and Least Significant Bit (LSB) Algorithm to hide secret images in grayscale cover image. This techniques implemented for improving security and imperceptibility and to avoid noise, sharpening and contrast of image. Initially, secret image was scrambled by Arnold Transform and concealed into cover image using Least Significant Bit (LSB). This algorithm is only applied and tested in BMP images. Experimentally this method improved good security and imperceptibility based on MSE and PSNR values. One drawback of the proposed work is little slow in extracting algorithm while add huge size images higher than 160*160 with different dimensions.

Das et al., (2015) [11] In this paper, authors implemented Cryptography and steganography are the two significant fields accessible for data security. While cryptography is a technique where the data is mixed in an unintelligent gibberish style during transmission, steganography centres on hiding the presence of the data. Joining the two spaces gives a more elevated level of security where regardless of whether the utilization of secretive channel is uncovered, the genuine data won't be uncovered. This paper focuses on hiding various secret images in a private 24-cycle cover image utilizing LSB replacement based image steganography. Every secret image is scrambled prior to loading away in the cover image utilizing Arnold Transform. Results shows proposed strategy effectively makes high capacity data keeping the visual nature of communicated image good.

3. PROPOSED ALGORITHM

3.1 Existing work

In this existing work, Image security has become one of the most significant problems due to the exponential growth of internet users. In many articles it tried to overcome the problem of high noises that might be placed on the image like a visible watermark.

- Mostly the boundary problem will affect the security, this means the pixel which is located for embedding will become unused, since it exceeds the maximum intensity level.
- In many existing works, Low-hiding capacity which is attributed to mainly hiding in smooth areas.
- Adaptive least significant bit is used in existing work, this method could be weak for hiding extra bits of signature with a hidden message for its integrity purpose.
- The noise sensitive area for embedding will lead high risk.

3.2 Least Significant Bit (LSB)

Least Significant Bit (LSB) technique is most ordinarily utilized for concealing data. In this technique the embedding is finished by supplanting the most un-critical pieces of image pixels with the pieces of secret data. The image got subsequent to embedding is practically like the first image in light of the fact that the adjustment in the LSB of image pixel doesn't bring an excess of contrasts in the image.

Algorithm

```
targetImageInGray=x1;
N = 3;
dataInDec = targetImageInGray;
dataInDecMasked = maskLast_N_bits(dataInDec, N );
givenLengthOfTextBits = bitStreamLength;
dataInDec_WithInsertedBits=insertIntoLSB_bits(dataInDecMasked, bitStreamOfImageToHide, N );
```

In the above algorithm, LSB technique is to mask every bit of secret image and hide into cover image. N gives the number of images to be masked.

3.3 Arnold Transform

Arnold transform is a sort of image scrambling approaches. The transformation shifts pixel position from (x, y) to (x', y') without changing its dark value. It is cyclic the secret image repeats itself after certain number of weights. The unique element of Arnold scrambling is that it utilizes periodicity indication. Figure 2, describes the process of Arnold Transform. Initially the original images is taken and key is inserted. By applying Arnold transform the image converted into block separation by 64*64 pixel, then Scrambled image is displayed.

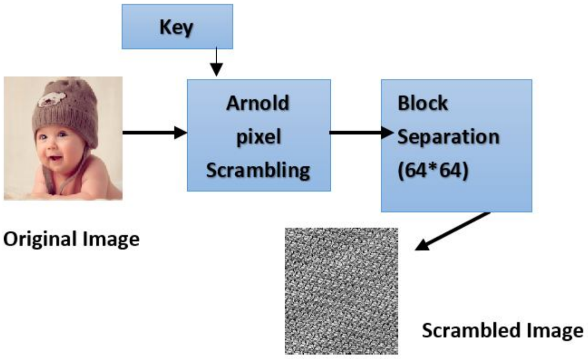

Figure 2: Process of Arnold Transform

The Arnold image transformation is defined as the point (x, y) in the unit square transforms into the other point (x', y')

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} * \mathrm{Mod}(N)$$

Here, x and y are the axes of the picture, Mod indicates the quotient and N is the length or breadth of the image. x' and y' are the picture co-ordinates.

3.4 Block Code Encoding

The Block Code Encoder module is proposed to anticipate input blocks of length eight openings, where a portion of these spaces are unfilled. These come from the PCM ENCODER module (in the 4-cycle mode). Block code encoding (BCE) is a coding plan that joins both adjustment and channel coding and depends on the Euclidean separation between images. This work represents how to develop a 4-QAM BCE code dependent on a 4-QAM signal star grouping with set dividing. The base Hamming separation is di, where 1 ≤ I ≤ 2. The two segment codes are utilized to build a 2 × N codeword exhibit by embedding the codeword ci of the ith part code Ci into the ith column of a 2 × N codeword cluster.

3.5 Proposed design

In this paper, proposed model is used to build security for images during transmission. This model develops two processes. The first is embedding and second one is extraction process. In embedding, Arnold transform is applied on secret image and get the mixed secret image. This process gives the greater security and strength to algorithm. Apply block encoded on the cover image and mixed secret image so as to build the security level. Here block code encoded to coefficients of particular sub-groups of cover image and mixed secret image. Block code encoded is block coded with LSB embedding to improve both the error correction ability and inserting payload. This factor is expanding the inserting quality factor. When the block encoding activity is done, stego image is produced using LSB algorithm. The decoding process is really the converse process of the inserting model which is extraction process. MATLAB R2016b platform is used to develop this model by combining these three algorithms LSB, Arnold Transform and Block Code Encoding. Figure 3. Shows the overall proposed design.

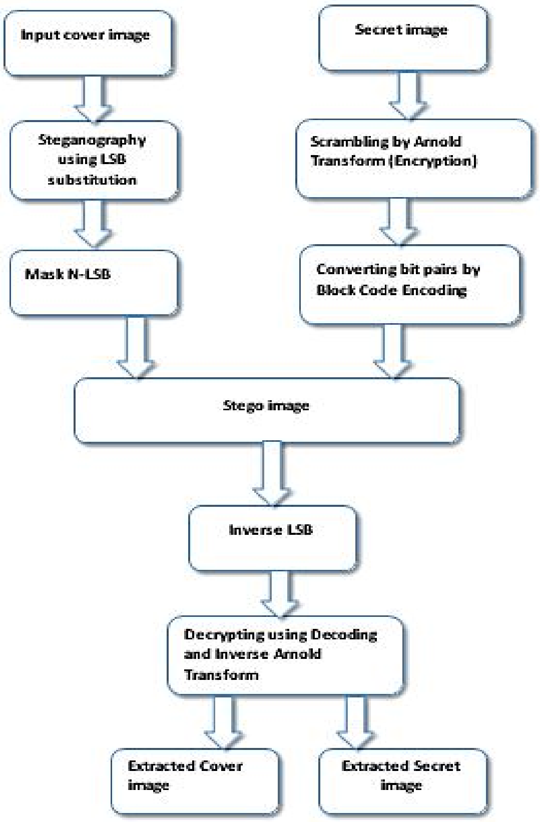
Input cover image
Secret image
Steganography using LSB substitution
Scrambling by Arnold Transform (Encryption)
Mask N-LSB
Converting bit pairs by Block Code Encoding
Stego image
Inverse LSB
Decrypting using Decoding and Inverse Arnold Transform
Extracted Cover image
Extracted Secret image

Figure 3: Proposed Design

3.6 Process

a. Pre-Processing

Pre-processing processes in the input picture employ a tiny pixel neighbourhood to get a distinct attributes were identified in the output image. All the pixels of an image are multiplexed by embedding strength factors alpha or beta. In this proposed model, pre-processing is apply for cover images size, contrast, brightness, and adjustments.

b. Embedding Process

Algorithm: Proposed embedding process

Input: Cover image CI, Secret Image SI

Step 1: Get and read the CI and check the constrains like size, contrast, brightness and etc.,

Step 2: Apply pre-processing on CI and Separated into RGB Channels

Step 3: Read the SI and convert secret image into grey scale image as SG

Step 4: By apply Arnold transform to SG and RBG of CI.

Step 5: Apply Block encoding to extract the coefficients of matrix CI and coefficient matrices

Step 6: Apply Arnold transform extract the coefficients of matrix CI

Step 7: Perform fusion operation on image to CI and SG to get fused image.

Step 8: Finally apply fused image with LSB process to form a stego image of SI.

c. Extraction Process

Algorithm: Proposed extraction process

Step 1: Receive the stego image and known cover image.

Step 2: Apply fusion process on both stego image and cover image to get fusion image.

Step 3: Apply Inverse LSB method to separate the Cover image and Secret images.

Step 4: From the recovered cover image, apply decoding process and Inverse Arnold Transform to get the decrypted secret images.

Step 5: Finally, Cover image and Targeted multiple secret images are extracted.

4. RESULTS AND DISCUSSION

The experimental results showed the efficiency of the proposed approach in terms of MSE and PSNR in decibels (dB) values.

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2$$

It can be computed by performing byte by byte comparisons of the cover image and stego image. Higher the value of MSE indicates dissimilarity between compared images.

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

It measures the stego image quality with picture cover. Higher PSNR implies higher the quality of image.It is measured in decibels (dB). An enormous PSNR esteem implies that the stego image is generally like unique image and the other way around. It is difficult for the Human eyes to recognize unique cover image and stego image when the PSNR proportion is bigger.

In this section, experimental results analyzed in terms of Embedding Capacity, Quality of the image and error between cover image and secret image. The Sample Test images are tested from the Dataset are USC SIPI database, Hlevkin and Cae.wisc.edu.

4.1 Embedding Capacity

From the figure 4, the embedding capacity of proposed work is compared with existing work. The Embedding capacity is high compared to existing work.

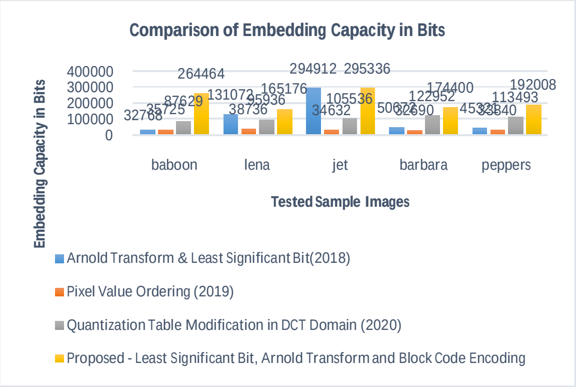

Figure 4: Comparison graph of Embedding Capacity (Bits) of Existing and Proposed System

4.2 Image Quality

From the figure 5, the quality of image for cover and secret image is calculated. Image quality is evaluated in terms of Peak Signal Noise Ratio (PSNR) which is measured in Decibels (dB). By comparing with existing work visual quality of image is good.

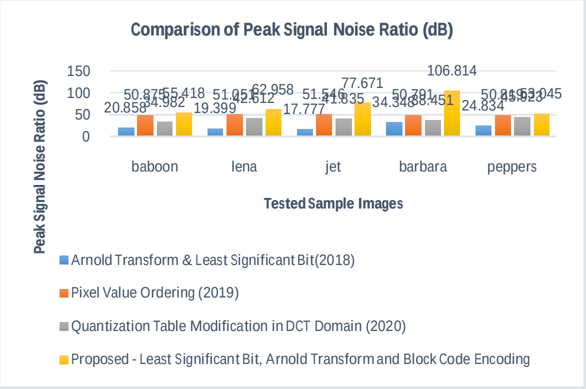

Figure 5: Comparison graph of PSNR (dB) of Existing and Proposed System

4.3 Error

From the figure 6, shows the error between cover image and stego image. The Maximum difference shows the high rate of error occurs and vice versa. From comparison with existing work, proposed work provides decrease of error.

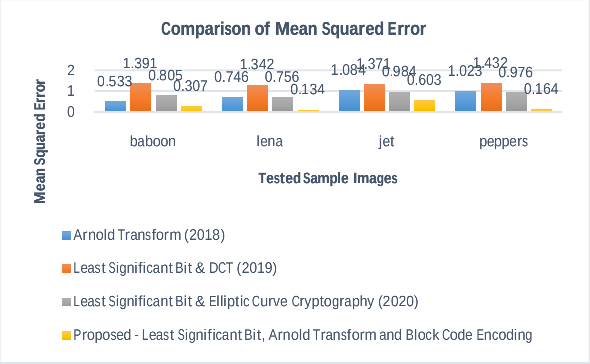

Figure 6: Comparison graph of Mean Squared Error of Existing and Proposed System

5. CONCLUSION

Steganography is the field of hiding data in manners that prevent credentials. In this paper secure steganography technique for inserting secret image into cover image has been proposed. The proposed work gives security and high limit-based steganography plan of concealing a huge size secret image into a little size cover image. Arnold transformation is applied to scramble the secret images. The steganography system is based on block code encoding and Arnold transform method to convert secret image into bit pairs to enhance security. The experimental results shows good performance compared to existing work in terms of numerical analysis i.e., PSNR and MSE. The proposed work provides better security, improved image quality and reduce error. The recommendation of future work is to enhance image, video and audio security in cloud environment based on different encrypting Techniques.

REFERENCES

1. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain**, "A New Approach for LSB Based Image Steganography using Secret Key"**, IEEE 14th International Conference on Computer and Information Technology, December 2011.
2. Altaay, A. A. J., Sahib, S. B., & Zamani, M. (2012, November). **An introduction to image steganography techniques.** In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp. 122-126). IEEE.
3. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). **Digital image steganography: Survey and analysis of current methods.** Signal processing, 90(3), 727-752.
4. P. G., B. R. and S. S**., "Dual Wavelet Transform Used in Color Image Steganography Method,"** IEEE, 2014 International Conference on Intelligent Computing Applications, Coimbatore, 2014, pp. 193-197
5. Liu, Hsing-Han & Lee, Chuan-Min. (2019). **High-capacity reversible image steganography based on pixel value ordering.** EURASIP Journal on Image and Video Processing. 2019. 10.1186/s13640-019-0458-z.
6. Dai HongzhuCheng JieLi Yafeng, **"A Novel Steganography Algorithm Based on Quantization Table Modification and Image Scrambling in DCT Domain"** · International Journal of Pattern Recognition and Artificial Intelligence, 2020.
7. Shanthakumari, R. and S. Malliga. **"Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm."** Multimedia Tools and Applications 79 (2020): 3975-3991.
8. Fouad, Osama & Hussein, Aziza & Hamed, Hesham & Kelash, Hamdy & Khalaf, Ashraf A. M. & Ali, Hanafy. **Hiding data in images using steganography techniques with compression algorithms.** TELKOMNIKA (Telecommunication Computing Electronics and Control). 17. 1168. 10.12928/telkomnika.v17i3.12230.(2019).
9. Maji, Giridhar, Sharmistha Mandal, Soumya Sen, and Narayan C. Debnath. **"Dual image based LSB steganography."** In 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), pp. 61-66. IEEE, 2018.
10. Sadik Ali Al-Taweel, Mohammed Husain Al-Hada and Ahmed Mahmoud Nasser. **Image in image Steganography Technique based on Arnold Transform and LSB Algorithms.**International Journal of Computer Applications 181(10):32-39, August 2018.
11. Das, Pallavi, Satish Chandra Kushwaha, and Madhuparna Chakraborty. **"Multiple embedding secret key image steganography using LSB substitution and Arnold Transfform."** In 2015 2nd International Conference on Electronics and Communication Systems (ICECS), pp. 845-849. IEEE, 2015.
12. Sharma, Vijay Kumar, Devesh Kumar Srivastava, and Pratistha Mathur. **"Efficient image steganography using graph signal processing."** IET Image Processing 12, no. 6 (2018): 1065-1071.
13. Jain, Aman**. "A Secured Steganography Technique for Hiding Multiple Images in an Image Using Least Significant Bit Algorithm and Arnold Transformation."** In International Conference on Intelligent Data Communication Technologies and Internet of Things, pp. 373-380. Springer, Cham, 2019.
14. Subhedar, Mansi S., and Vijay H. Mankar**. "Image steganography using contourlet transform and matrix decomposition techniques."** Multimedia Tools and Applications 78, no. 15 (2019): 22155-22181.
15. Wafaa Hanna Zaki Sharaby**, "Improving Image Steganography using a Proposed Mutated Levy-Flight Firefly Algorithm"**, International Journal of Computer Applications (0975 –8887)Volume 182– No. 20, October 2018.
16. Edi Jaya Kusuma, Christy Atika Sari, E**, "A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography"**, Journal of ICT Research and Applications, 2018.
17. Thakre, Ketki, and Nehal Chitaliya. **"Dual image steganography for communicating high security information."** International Journal of Soft Computing and Engineering (IJSCE) 4, no. 3 (2014).