Digital color image steganography for nonspecific format and secured based on Clustering

Mohamed Tahar Ben Othman,
Senior Member of IEEE
Computer Science Dept, College of Computer Qassim University Saudi Arabia
B.I.N.D. research group

Arshiya Sajid Ansari,
Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Saudi Arabia

Mohammad Sajid Mohammadi
Information Technology Department, College of Computer Qassim University, Saudi Arabia.

Abstract:
We are presenting a more secured and nonspecifically dependent on image formats steganography technique for any bmp or JPEG digital images, based on clustering technique. It is a new color image clustering technique used for robust steganography. It can be defined as the persistence of the embedded steganography under image unrests resulting from attacks. Firstly, the image under consideration is divided into 8x8 blocks and then the clusters of blocks, using the Content Addressable Method (CAM). The cluster of blocks is divided into sub-clusters and Payload data are embedded into next level of cluster i.e. sub clusters. Duplication of the same payload data has been achieved through these sub-clusters which prove the robustness of our proposed steganography technique. Moreover, the distribution rate of image sub-clusters over a cluster it is another parameter that can be tuned to improve this robustness. We used this technique and proved with bmp images in previous works and it showed promised results. In the presented work, this technique has been applied on JPEG image coefficient level. Experimental results indicate that if we have more rate of dispersal of clusters on the image with Block/pixels more uniformly distributed of throughout the clusters, the best robustness of steganography we could obtain. This result comes from the fact that the proposed technique resists to geometric attacks like cropping of stego image.

Key-Words:
Steganography, Distribution Rate, Color Images, Content Addressable Method. Cluster Dispersal Rate

1. Introduction

The key requirements of steganography i.e. information hiding are robustness and imperceptibility. There are many algorithms on steganography but very few are providing multiple image format support and good security against attacks. In present work we are providing the concept of clustering for hiding data to implement generic steganography. Image clustering has gained good attention in IP domain. Clustering is used for images classification [1] in many classifiers such as Neural Network, Markov model, linear classification Bayesian. Our main Idea is focused on Content Based Image Retrial (CBIR) [1, 2]. These classifiers are generally used in Image retrieval system from an image dataset. Color image clustering technique has been used in the image segmentation domain or pattern recognition and alike. It is better idea to segmentation the image for retrieve information from the image itself [3-6].

This work presents a new secured steganography technique which can support more than one image formats and uses new method of clustering based on the Content Addressable Method (CAM) which was introduced in [2,7]. Unlike other steganography/ watermarking methods the aim of this method is not only data hiding but also provide good security robustness with multi format support. In cover image clustering each of the cluster contains all coefficient coordinates of it that have the same address generated by selected function for clustering. Then these clusters are divided into many sub-clusters in each one. Each sub-cluster is embedded with the same portion of data from the pay load data to be hidden.

The reaming sections of this paper are as follows. Section 2 presents the related works, section 3 describes Block Clustering Vs Pixel Clustering, section 4 has Proposed Steganography Scheme in details while section 5 gives experimental results and detailed analysis. In section 6 presents the conclusion and future work.

2. Related works

We discuss in this section some of the studies in steganography. It also discusses some used techniques of clustering in steganography/watermark scheme.

Manuscript received April 5, 2019
Manuscript revised April 20, 2019

In [8] an image steganography has been proposed with a lossless steganography approach mainly based on clustering and contouring on monochrome image only. The results show better data hiding capability with improved perceptibility of stego image. It shows that authors have enhance the stego image PSNR value. The stego image quality has been compared with other similar works. As per the author point of view they claim that the results of their work is better than other works, it is more realistic and straight forward for steganography applications.

In work [9], for fast image transfer and good security in transmission, a scheme is developed based on effective elapsed time. This work is divided mainly into three parts: the compression, the encryption and the steganography. The encryption is done using blowfish algorithm and a robust compression is built using a modified DWT compression. It provides better security mechanism for sharing of images over the social media apps. Two important parameters: signal to noise ratio (PSNR) and mean squared error (MSE) are observed and evaluated along with Compression Ratio (CR), and Elapsed time (ET). They claim that their overall system performance is more robust, fast and effective as far as image security is concerned. The work is tested on six data set of classified images. All have good results. Some improvement is possible for quick results and could be compare with different data set.

The proposed work in [10] is a cryptography technique using the algorithm cohort intelligence (CI) conveyed to as Improved Cohort Intelligence (ICI) is proposed. The approach of ICI is mainly based on the two properties of candidates. To implement reversible data hiding ICI algorithm has been tested over JPEG images for steganography. They have used 256×256 grey scale image size in both the 2 quantization tables of size 8×8 and 16×16. Experimental results validate in the computational cost of the proposed work. The computational time is reduced 77% which is significantly good improvement. Similarly, with 16×16 quantization table, the computational time with ICI method is reduced by a minimum of 53% and a maximum of 91% as compared to cohort Intelligence with Cognitive Computing (CICC) and a minimum of 62% and a maximum of 87% as compared to Modified-Multi Random Start Local Search (M-MRSLS).

Image quality and payload capacity have also been improved in some cases by using 16 ×16 quantization table. However, they did not do steganalysis [11] to verify the security aspect of the work presented. The improvement is possible by the optimization algorithms in machine learning based steganography or deep steganography [12].

In [13], theories of cryptography and steganography that exist in previous researches have been combined and author had provided a small development with optimal results. To improve imperceptibility of stego images author has used LSB technique on cover image edge area only. The PSNR and MSE show that imperceptibility values are better than those of previous studies. Histogram analysis also done for original and stego images and proved that proposed method is working better. Here messages are encrypted by converting to binary forms hence results in more verbal message encryption, thus minimizing the chance of messages being destroyed by unauthorized parties. This is evidenced by correlation coefficient (CC) of encrypted message. The CC value for extracted encrypted message is 1 which means there is no data loose. The disadvantages of this work is that author did not do analysis of attack like cropping of the stego image. Also by inserting payload in the image edge area, the payload data capacity is very less as it is depending on the number of edges area in the image.

In work [14,15] the author has done extensive survey of recent steganography techniques for multiple image formats Jpeg, Bmp, Tiff, and Png image formats and has discussed the file structure of each image formats. Also, the work discussed the application and limitation of steganography techniques. Authors have shown the classification of steganography methods based on the formats of the images and their encoding domain. Finally, they discussed the steganalysis process in general with some tools like Ben4D, Openpuff, StegoDetect, F5, Comouflag, JPegX and StegExpose Ben 4D.

In work [16], authors have present a scheme of clustering modification directions (CMDs). This scheme reduces the steganalysis detection chances by taking benefit of the changes that occur due to embedding. Their CMDs novel strategy is based on the assumption that is given in [16] “when embedding changes are in heavily textured area and are locally heading toward the same direction, the steganographic security might be improved”. They have implemented this approach by dividing the cover image into some sub-images, where payload data segments are embedded with some steganography schemes that are well-known by using additive distortion functions. Dynamically costs of each pixel are considered and updated to take benefit of mutual embedding impacts. If the neighbor pixels are changed in either direction, the cost is biased toward the same direction. Experimental results showed that using the strategy CMD added to the existing schemes of steganography, can overcome, effectively and with high dimensional features, the challenges of modern steganalyzers.

Lingling et al. have proposed in [17] the Statistical Quantity Histogram (SQH) shifting algorithm based on clustering to build a novel watermark scheme to show low run-time complexity better robustness. Their research output performance was good with regard to robustness and reversibility. They target, mainly, different kind of attacks’ masking models.

In paper [18], Yan Haowen’s watermarking approach uses the concept of shuffling of the cover image, extracting the feature to form the clusters of points of the data to embed

the watermark in the LSBs of pixel value. The main aim is to govern and protect the copyrights. But author did not do much experimental testing.

A new enhanced watermarking algorithm based on singular value decomposition and kernel fuzzy clustering in the complex wavelet transform domain is proposed in work [19]. Authors have used complex wavelet transform to decompose the cover image. Data is embedded in low frequency coefficients then 2 properties of stego image: high-frequency texture features image and low-frequency background are used as fuzzy clustering feature vectors. This way the strength of embedding is found. This approach gives good resistant to different kinds of attack. They did some testing of image rotation where the correlation has change from 0.93 to 0.98 based on the image.

In the work [6] we proposed a new clustering approach for colored images called Content Addressing Method (CAM). The built clusters and sub-clusters are used to embed and extract the watermarks into and from the image. The aim of the work in [6] was to prove the robustness of the proposed scheme against rotation attacks. The results showed good results using bmp image format.

3. Block Clustering vs Pixel Clustering

The image clustering is done in two ways: for JPG images is done at the level of coefficients blocks while at BMP images is done at the level of pixels. In this paper we focus on the Block Clustering. The Pixel Clustering is studied in details in our previous works in [2,6,7]. In the Pixel Clustering, a set of pixels having the same features are declared to be in the same cluster. These features are used to address this group of pixels. With the same technique, in the Block Clustering, a set of features are used to regroup a set of blocks in the same cluster. In this new technique of clustering, the blocks or the pixels of the same cluster might be potentially scattered from each other in different geometric areas in the cover image. Each sub-cluster is used to duplicate the embedded data which helps adding robustness against attacks. Like it was mentioned in our paper [6] if the rate of the distribution of pixels over clusters area is high the robustness against attacks is also high. In the proposed framework, the function providing the cluster address is taken from the left-upper corner of each block 8x8 of the JPEG coefficients as shown in Fig. 1.

-3	123	-21	8	0	1	1	0
4	-3	0	3	1	0	1	0
2	-1	0	1	0	1	0	0
0	0	1	0	0	0	1	0
2	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Fig. 1 Features in the JPEG Coefficients Block

Depending on the choice, which is taken as parameter to our clustering technique, a function of one to four values in this corner forms the address. The function in Fig. 2 gives the cluster address. To get more blocks in a cluster, the least significant bits for each value are stripped out.

```
clusterAdd(nbfOfValues, lsbStripped, block)
        coord=[(1,1),(1,2),(2,1),(2,2)];
        address=0;
        for i=1: nbfOfValues
          address = address<<(8- lsbStripped)+
          abs(block(coord(i)(1), coord(i)(2))) &
          (0xff<< lsbStripped);
        end
        return address;
end
```

Fig. 2 Function of address of s cluster

The parameters of this function, the number of chosen values and the LSB stripped bits, are part of the key of the used steganography technique.

A cluster may contain a number of blocks. Every cluster is divided into sub-clusters with the same size (*nbpsc* blocks) except the last one which may contain between *nbpsc* and 2* *nbpsc* -1 blocks. To address a sub-cluster into a cluster a counter is maintained in the right-bottom corner of the block which is shown in green values in Fig. 3. The data is then embedded into the same corner as it is shown in the remaining highlighted values in Fig. 3. The number of bits used for the counter and for the embedded data and the mapping function for each are the second part of the key of the steganography technique.

2	6	7	1	1	1	0	0
9	6	0	0	-1	1	0	0
0	-3	0	-2	-1	0	0	0
-3	0	-2	-2	0	-1	0	0
0	0	0	0	0	0	0	0
-1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Fig. 3 Sub-cluster counter and embedded data

The function inserting the sub-cluster counter and embedding the data is given in the algorithm described in Fig. 4.

```
blockEmbedd (scCounter, data, block)
        cCoord=[(6,8),(7,7),(8,6)];
        dCoord=[(7,8),(8,8),(8,7)];

        for i=1: 3
          block(cCoord(i)(1), cCoord(i)(2)) =  scCounter (i);
          block(dCoord(i)(1), dCoord(i)(2)) =  data(i);
        end
end
```

Fig. 4 Function of inserting sub-cluster counter and data

The order of inserting the counter and embedding the data is a function that forms a third part of the key of the steganography technique.

4. Proposed Steganography Scheme

4.1 Steganography Scheme algorithm

The proposed steganography scheme is given in Fig. 5. It starts by determining the clusters in the cover image, then every cluster is divided into sub-clusters while data is being embedded. The Key is describing the number of values forming the cluster address, the number of least significant bits stripped from these values and the way to concatenate these values to form the address, and the way to insert the sub-cluster counter and to embed the data. The third step for this algorithm is formed by the attack of the stego image. In this paper, we consider only cropping attacks. The fourth step is the reverse the process starting by a new clustering of the attacked image which is followed by the stego-data extraction using the steganography key.

```
Steganography_Algorithm ()
{
   clusters_set = clusterize(cover_image);
   embed_data(cover_image, data, clusters_set)
   attack(stego_image);
   clusters_set = clusterize (attacted _stego_image);
   extraction_of_data ( attacted _stego_image,cluster _set);
}
```

Fig. 5 Steganography Algorithm Scheme

4.2 Embedding Phase

After cover image's clustering, the image is indexed using the cluster address. All blocks having the same address belong to the same cluster. The number of blocks in the cluster is divided into equal size sub clusters. A sub-cluster's blocks are then used to hold the same information or data. This data duplication over a distributed area of the image is increasing the level of robustness of our steganography proposed technique. The embedding algorithm is given in Fig 6.

```
embed_data(cover_image, data, clusters_set)
{
   For each cluster in clusters set:
    For each block in the cluster:
        blockEmbedd(scCounter,data,block)
}
```

Fig. 6 Embedding Phase

Depending of the settings defining the way to form the address and the way to insert the sub-cluster counter and to embed the stego data that are described in the key, the data will be securely embedded.

4.3 Extracting Phase

Fig. 8 gives the algorithm of the extracting phase. This phase starts with a new clustering process using the settings carried in the key. The image is then indexed using the clusters' addresses. The data should be extracted in sequence from the clusters going from the first until the last address. Inside the cluster, the same process is followed: data is collected in sequence from the sub-cluster 1 until the maximum number of sub-clusters in the cluster. A block having a counter 0 is not used for data embedding.
A Lookup Recover Table (LRT) is given in Fig. 7 used to handle all duplicated data in the same sub-cluster.

corrupted data	0	1	1	0	0	0	1	0	0
	0	1	1	0	1	0	1	0	0
corrupted data	0	0	1	0	1	0	0	1	0
lost data	0	0	0	0	0	0	0	0	0
	0	1	1	0	1	0	1	0	0
recovered data	0	1	1	0	1	0	1	0	0

Fig. 7 Lookup Recover Table

If the maximum values in a column are 0s then the recovered bit is considered 0 otherwise it is 1.

```
data = extract_watermark(image, clusters_set)
{
 For every cluster in clusters_set
      For every sub_cluster  from cluster
        For each block in sub_cluster
          add_data2LRT()
          data ← recoverData(LRT)
}
```

Fig. 8 Extracting Phase

5. Experimental Results and Analysis

The steganography is generally used to secure the embedded data while watermarking is used to secure either the embedded data or the cover image or both. While the

main goal of steganography is carrying a secure data into a digital image, the sender is not pushed to use specific cover images but should choose which can easily carry the data to be sent securely. For this reason, our proposed technique is providing the number of clusters, sub-clusters and the data size that can be carried out. We used a set of color images shown in Fig. 9 with a size 512×512×3 as a cover images and 64×64 binary image given in Fig. 10 as the stego data which comes to text of 512 characters.

We are using two main performance measurement tools: the correlation coefficient (CC) given in equation (1) to measure the similarities between the embedded and extracted stego data:

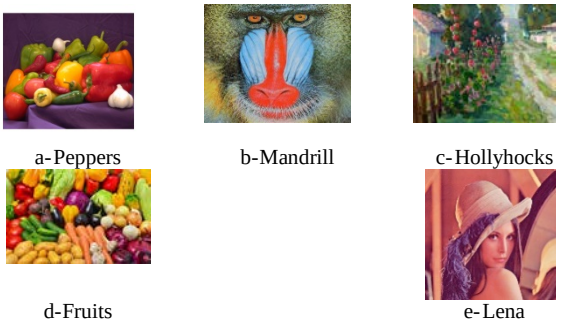
$$CC = \frac{\sum_x \sum_y osd(x,y) esd(x,y)}{\sum_x \sum_y osd^2(x,y)} \qquad (1)$$

Where *osd* is the actual stego_data and *esd* is the extracted stego_data.

The Peak Signal to Noise Ratio (PSNR) is used to evaluate the difference between original image and the stego image. Equation (2) provides the formula of the PSNR:

$$PSNR = 10 \log \left(\frac{\max\left(ci^2(x,y)\right)}{\frac{1}{MxN} \sum_{y=1}^{M} \sum_{x=1}^{N} \left(ci(x,y) - si(x,y)\right)^2} \right) \quad (2)$$

Where *ci* is the cover image and *si* is the stego_image.



a-Peppers b-Mandrill c-Hollyhocks

d-Fruits e-Lena

Fig. 9 Cover images set

Copyright image

Fig. 10 Stego data

Fig. 9 and Fig. 10 gives respectively the cover images and the Stego Data image.

The Table 1 presents the number of clusters, sub clusters, and maximum size of the data that can be embedded over different cover images. These statistics are collected using a key that takes only one value in the upper-left corner (ULCV) of a block as the cluster address after stripping the least significant bit and a maximum counter value of 4 blocks in each sub-cluster and 9 bits of data embedded in the three positions in the bottom-right corner of the block.

Table 1: Statistics of the cover image with ULCV=1

cover image	number of clusters	number of sub_clusters	max. size of stego_data(bits)
Lena	179	1305	12255
Fruits	46	250	2403
Hollyhocks	42	249	2382
Mandrill	67	81	840
peppers	49	52	540

Modifying only the number of values in the upper-left corner from 1 to 3 for the cluster address gives some better solutions as shown in the Table 2.

Table 2: Statistics of the cover image with ULCV=3

cover image	number of clusters	number of sub_clusters	max. size of stego_data(bits)
Lena	331	1150	10974
Fruits	102	532	5023
Hollyhocks	73	607	4902
Mandrill	17	57	305
Peppers	29	38	372

The normal visualization or perceptibility of cover image is not affected by the proposed solution which is supported by the PSNR values shown in table 3.

Table 3: PSNR of cover image

	JPEG Coefficients	BMP Spatial[2]
Lena	47.04	NA
Fruits	47.93	NA
Hollyhocks	41.07	44.00
Mandrill	59.81	44.68
Peppers	62.21	41.56

The PSNR of the images Mandrill and Peppers are very high as only a small portion of the data is embedded because of the reduced number of sub-clusters in these images. The first three images are able to hold all the stego data and still the PSNR is high.

5.1 Blocks Dispersal Rate

As we proposed in [6] for the pixels in a cluster, we used the blocks distribution over a cluster in this study as the area covered by the cluster's blocks in the cover image. Furthermore, we consider the sub-cluster – holding the same data – dispersal rate (SCDR) shown in the equation 3 as the area covered by the sub-cluster's blocks over the area of the cluster.

$$\mathrm{SCDR}_c = \frac{(x_{max_{sc}} - x_{min_{sc}}) * (y_{maxs_c} - y_{min_{sc}}) * 100}{(x_{max_c} - x_{min_c}) * (y_{max_c} - y_{min_c})}, \qquad (3)$$

Fig. 11 gives the cluster distribution rate of the clusters in Lena with one address value and one LSB bit stripped out.

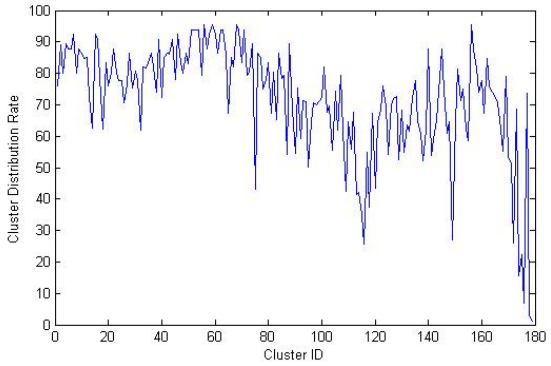


Fig. 11 Lena-Cluster Distribution Rate

Fig. 12 presents the number of sub-clusters per cluster in Lena with the same settings.

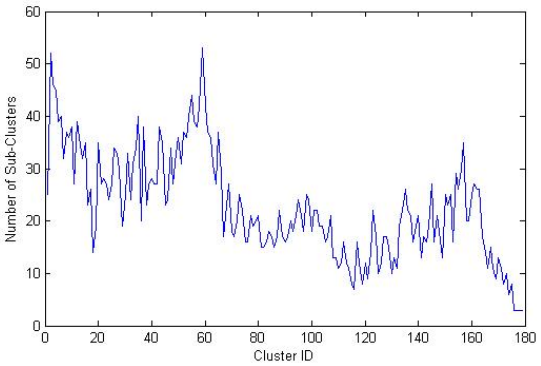


Fig. 12 Lena-Number of Sub-Clusters per Cluster

Fig. 13 provides the SCDR in Lena with the same settings.

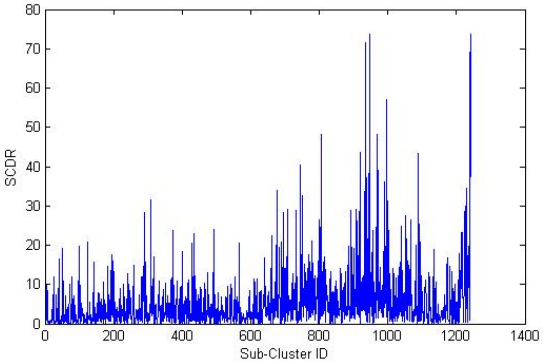


Fig. 13 Lena-Sub Clusters Dispersal Rate

The sender can run using different settings to choose which is the best image and configuration that may hold the stego data with the best distribution. The settings are then sent with the steganography key. Moreover, depending on the stego data size, the sub-clusters that have a reduced SCDR may not be used.

Fig. 14 Cropped images

For the images that can hold the stego data or a considerable part of it and without attack, the stego data is extracted without any lose (NC =1). We cropped the images as showed in Fig. 14 after being embedded with the stego data. The NC of the extracted data is shown in Table 4.

Table 4: NC affer cropping

Cropped Image	NC of extracted data
Lena	1
Hollyhocks	0.97
Fruits	0.95

The data is not affected when using Lena as cover image because the number of sub-clusters is considerable with high SCDR. The crop may happen in an area that contains entire sub-clusters which may result on lose of data. For this reason, the sender can decide of using only the sub-clusters that have high SCDR and then report this decision in the transferred key.

6. Conclusion

In this work digital color image steganography on nonspecific format and secured based on Clustering and Content Addressable Method (CAM) is proposed. This clustering technique is aimed to be used for the steganography in color images of different formats. The cover image is divided into a set of blocks grouped in a set of cluster and sub-clusters which are built over Content Addressable Method. Each sub-cluster is used to hold the exactly same data portion from payload data. The achievement of this work is that it supports many image formats and it is robust as proved through the achieved results. Also security is provided through multiple portion of key in the secure embedded key. Our experimental results witness of the fact that if SCDR value is high we obtain better results.

Acknowledgment: This work is supported by Scientific Research Deanship of Qassim University Saudi Arabia under the Project ID: 2029-coc-2016-1-12-S. The authors are highly thankful of SRD Qassim University for such support.

References

[1] Wangming X, Xinhai L, Kangling F. “Content-based image clustering via multi-view visual vocabularies”. In Proceedings of the 31st Chinese Control Conference 2012 Jul 25 (pp. 3974-3977). IEEE.

[2] Othman MT. “New Image Watermarking Scheme based on Image Content Addressing Method”. In13th WSEAS International Conference on Applied Computer and Applied Computational Science ACACOS 2014 Apr (Vol. 14, pp. 23-25).

[3] Chaudhry A, Hassan M, Khan A, Kim JY, Tuan TA. “Image clustering using improved spatial fuzzy C-means”. In Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication 2012 Feb 20 (p. 86). ACM.

[4] Shukui Bo, Yongju Jing, "Image Clustering Using MeanShiftAlgorithm", Fourth International Conference on Computational Intelligence and Communication Networks (CICN), 2012, DOI: 10.1109/CICN.2012.128, Publication Year: 2012 , Page(s): 327 – 330.

[5] Singh, D. ; Singh, A. ," A New Framework for Texture Based Image Content with Comparative Analysis of Clustering Techniques", Fourth International Conference on Computational Intelligence and Communication Networks (CICN), 2012, DOI: 10.1109/CICN.2012.22, Publication Year: 2012 , Page(s): 232 – 236.

[6] Othman M.T., “Novel image clustering based on image features for robust reversible data hiding”. International Journal of Fuzzy Systems and Advanced Applications. 2015:1-8.

[7] Othman M.T. “CAM-based Digital Image Watermarking Revisited”. WSEAS Transactions on Systems. 2014 Jul;13: 510-9.

[8] Manikandan G, Krishnan RB, Kumar NR, Narasimhan D, Srinivasan A, Raajan NR. “Steganographic approach to enhancing secure data communication using contours and clustering”. Multimedia Tools and Applications. 2018 Dec 1;77(24):32257-73

[9] Brar SS, Brar A. “Double layer image security system using encryption and steganography”. International Journal of Computer Network and Information Security. 2016 Mar 1;8(3):27.

[10] Sarmah DK, Kulkarni AJ. “Improved Cohort Intelligence—A high capacity, swift and secure approach on JPEG image steganography”. Journal of Information

[11] Akhtar, N., Khan, S. and Johri, P., (2014), February. “An improved inverted LSB image steganography”. In Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on pp. 749-755. IEEE.

[12] Denemark, T., & Fridrich, J. (2017). “Steganography with Multiple JPEG Images of the Same Scene”. IEEE Transactions on Information Forensics and Security.

[13] Irawan C, Sari CA, Rachmawanto EH. “Hiding and securing message on edge areas of image using LSB steganography and OTP encryption”. In2017 1st International Conference on Informatics and Computational Sciences (ICICoS) 2017 Nov 15 (pp. 1-6). IEEE.

[14] Ansari AS, Mohammadi MS, Parvez MT. “A Comparative Study of Recent Steganography Techniques for Multiple Image Formats”. International Journal of Computer Network and Information Security. 2019;11(1):11.

[15] Ansari AS, Mohammadi MS, Parvez MT. “JPEG Image Steganography based on Coefficients Selection and Partition”. International Journal of Image, Graphics & Signal Processing. 2017 Jun 1;9(6).

[16] Li B, Wang M, Li X, Tan S, Huang J. “A strategy of clustering modification directions in spatial image steganography”. IEEE Transactions on Information Forensics and Security. 2015 Sep;10(9):1905-17.

[17] L. An, X. Gao, X. Li, D. Tao, C. Deng, J. Li, “Robust Reversible Watermarking via Clustering and Enhanced Pixel-Wise Masking”, IEEE Transactions on Image Processing, Vol.21 , Issue: 8, DOI: 10.1109/TIP.2012.2191564, Publication Year: 2012, pp. 3598-3611.

[18] Yan H. “Watermarking algorithm for vector point clusters”. In 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing 2011 Sep 23 (pp. 1-4).

[19] Fan J, Wu Y. “Watermarking algorithm based on kernel fuzzy clustering and singular value decomposition in the complex wavelet transform domain”. In 2011 International Conference of Information Technology, Computer Engineering and Management Sciences 2011 Sep 24 (Vol. 3, pp. 42-46).

Mohamed Tahar Ben Othman Is a Professor of computer science since November 2017 and head of B.I.N.D. research group, Associate professor from October 2010 until November 2017, he received his Ph.D. in Computer Science from The National Institute Polytechnic of Grenoble INPG France in 1993, His Master degree in Computer Science from ENSIMAG "École Nationale Supérieure d'Informatique et de Mathématiques Appliquées de Grenoble" in 1989. He received a degree of Senior Engineer Diploma in Computer Science from Faculty of Science of Tunis. He became a Member (M) of IEEE in 1997, and a Senior Member (SM) in 2007. He worked as post-doc researcher in LGI (Laboratoire de Genie Logiciel) in Grenoble, France between 1993 and 1995, Dean of the Faculty of Science and Engineering between 1995 and 1997 at the University of Science and Technology in Sanaa, Yemen, as Senor Software Engineer in Nortel Networks, Canada, between 1998 and 2001 and Assistant Professor in Computer College at Qassim University in Saudi Arabia from 2002 until October 2010. His research interest areas are information security, wireless networks, Adhoc Networks, communication protocols, and bioinformatics.

Mrs. Arshiya Sajid Ansari has received her B.E degree in Computer Technology from the Yashwantrao Chavan College of Engineering, Nagpur University, India and M. Tech. in Computer Engineering from the NMIMS University, Vile Parle Mumbai, India. She is Ph.D. from Noida International University NCR Delhi Noida, India. She has 9 years of experience in teaching field. She is currently working as an assistant professor at Majmaah University Saudi Arabia. Her research areas of interests are image processing and data warehousing. She is a lifetime member of ISTE.

Mr. M. Sajid Mohammadi has completed his B.E degree in Computer Technology from the Yashwantrao Chavan College of Engineering, Nagpur University, India. He did his M. Tech. Computer Engineering from the NMIMS University, Vile Parle Mumbai, India. He is pursuing his Ph.D. from Noida International University NCR Delhi, India. He has total 16 years of experience including 1.5 years industrial experience in Reliance Petroleum Mumbai and 13.5 years of teaching experience. He is currently working as Lecturer in Computer Engineering Department, Qassim University Saudi Arabia. His research interest includes
Image Processing, Information Hiding, and Information/Network Security. He is a member of Saudi
Internet Scientific Society for the year 2017-18.