

Enhancing Network Security for Image Steganography by Splitting Graphical Matrix

Rohit Kumar*, Kamaldeep Joshi**

Department of Computer Science & Engineering, U.I.E.T, Maharshi Dayanand University, Rohtak (Haryana), India
e-mail: *rohitahlawat812@gmail.com, **kamalmintwal@gmail.com
Corresponding Author: rohitahlawat812@gmail.com

ORCID ID: 0000-0002-3801-6599*, 0000-0002-3238-0234**

Research Paper Received: 26.08.2019 Revised: 21.10.2019 Accepted: 15.01.2020

Abstract—The proposed work has focused on the security of image in order to save it from external attacks. However, there have been several existing steganography mechanisms to secure the graphical contents, but there are still threats from external attacks. Moreover, in case of bulky image it becomes difficult to shift content over a network without any loss. Thus proposed work has been introduced to allow graphical splitter mechanism to break graphical content in multiple parts by splitting image matrix in two or multiple parts according to image size. If the image size is less bulky, it could be split into just two parts or if the image size is more bulky, it could be split into more than two or multiple parts. This would save the image from being hacked or read in unauthentic manner. The proposed work would apply a key to divide image matrix in two or more than two parts so that it could not be easily understood. The proposed work also concentrated on Threats to security, Nature of attacks and delay in pre-processing. It also focused on delay during the process of encryption and decryption, image quality. Moreover, there are several compression techniques to compress the graphical contents to increase the transmission speed. The proposed work has compared traditional compression mechanism with present splitting mechanism that would reduce the size of the image along with providing security.

Keywords—Steganography; Encryption; Image processing; Image compression.

1. Introduction

Digital image processing has been considered a process in which the computer algorithms are used in the field of computer science. It is applied to carry out the processing of image on digital graphics. Digital image processing (DIP) has been considered a subcategory of digital signal processing. It has numerous features in analog image processing. It provides us a huge package of algorithms. These algorithms are useful on input data. It has the efficiency to minimize the challenges. These challenges

may be the build-up of noise and signal distortion. These issues grow up when the image processing take is executed. The images are defined over two dimensions. There is the possibility that these dimensions are either two or more. The digital image processing is modeled as systems. These systems have many dimensions.

The phase “Network security” is showing the meaning of itself. This phase, meaning is the security of the network. It has been considered an activity. It is created in order to protect the uses

and integration of network along with data. The hardware equipment as well as software equipment have same importance in the security of the network. An efficient network security system is capable to manage the complete network. It carries an objective. The objective is that it observes all threats. It avoids the network to enter or spread on the network.

Encryption is a process. This procedure encodes the message or information in a specific manner. After the encryption of data, merely the authority obtained person can achieve the data. In encryption, the plaintext is the simple message or information. Encryption algorithms are used to encrypt the plain text. The cipher is an encryption algorithm. It secures the data by converting it into cipher text. It can be understood only after the decryption.

Normally the pseudo-random encryption key is applied to resolve the technical challenges. It has been created using an algorithm. According to principle, it is impossible to do the decryption of data without possessing the key. On the other side, it has been proved that the capable computational resources with skills are required to create an efficient encryption system. Only authorized recipients will have the capacity of decryption of data. The decryption will be with the key.

Decryption is working similar with small changes. Thus, the key is applied for decryption of a block of information. After that the information will work again with initialization vector. The plain text is decrypted form of the cipher text.

Steganography

Steganography is the technique in which we hide some confidential data or information with ordinary information and extract that hidden information at its target point [1]. Steganography is the technique comprised of an art and science with practice. In

this technique, the sensitive data that can be any information or image, etc. is securely hidden in any other data (information, files or images etc.). This theory of steganography is not any new method or idea. For millennia, we have been hiding the information using the things of daily usages. Initially, as an example, watermarking was used on confidential and copyrighted memorandums, engravings in the underlying sides of the tables using some other methods. But nowadays, this theory of steganography has been utilized with digital facilities [2].

The concept of visual cryptography based on same theory is utilized on images. This technique can also be used anyway, or with anything, so should not be believed without having any knowledge or understanding of the same. If any image is obtained by any malicious person, that image would be of dreadful creation or casual noise. But generally in forensic labs, such noise could be decrypted effectually and could be an important proof in any criminal case.

2. Literature Review

There are several researches related to image steganography. Some of them have been described here:

In 2015, Vinay Kumar Pant et al. [3] proposed three step data security model. This model is capable to use in cloud computing. The proposed system is based on RSA. The research work described the way by which the security of the data can be achieved. For this purpose the proposed cryptography with steganography methodology has been utilized.

In 2015, Randeep Kaur et al. [4] reviewed on cloud computing security challenges with solution. Transmission information performs a considerable role in the daily life of us. Therefore the security

of information is very essential to be considered. The research work has highlighted the obstacles regarding the safety of cloud computing. The security techniques are described here in order to decrease the issue in regard to cloud computing.

In 2017, B. Fathima Mary et al. [5] analyzed the Data Security Enhancement in Public Cloud Storage Using Data Obfuscation and Steganography. For this purpose the data obfuscation with steganography is used. In the research work an elegant and novel technique has been presented. It has been done to increase the data security.

In 2017, Ataussamad et al. [6] evaluated the improvement of steganography. Here K strange point clustering has been used. The research work has emphasized on security of information when making use of cloud computing with proving that the technique with K Strange Points Clustering Algorithm performs better than K Means Clustering Algorithm.

In 2018, Ahmed A. Abd El-Latif et al. [7] presented a secure Quantum Steganography Protocol. The area of research is fog and IoT. For this purpose, a well-designed security technique is discussed here. In the research work, a new schema to keep the data safe in fog cloud IoT is presented. The proposed protocol is capable to defeat the different types of attacks. The discussed concept has been proposed to be used in mobile edge and fog computing.

In 2019, Jishen Zeng et al. [8] wrote on WIS-ERNet. It has been used for Steganalysis of Color Graphics. In the results it has been clear that the proposed network outperforms. To fulfil the purpose, the efficiency of detection is achieved. The process of proposed work is executed with less than half the complexity.

In 2019, Yuileong Yeung et al. [9] stated safe binary graphic steganography. It has relevancy with prediction. In this research work, the binary graphic

steganographic system has been proposed here. It has the objective to minimize the embedding distortions. Such has been measured using prediction. In order to play the advantage of distortion measurement, the research work has been done.

In 2019, Aya Y. AlKhamese et al. [10] introduced data protection in cloud computing. In the research work the steganography has been offered. In the research work many graphic steganography methods are used to hide the data in graphic.

In 2019, Aurijeet Mukerjee et al. [11] stated the research work to enhance the remembrance of Password in a graphic. The research work has focused on altering the system. It includes the 'text' as a password. The reason is that the mostly person cannot remember their passwords. It is well known thing that it is easy to keep in mind the picture, instead of the text.

In March 2019, Vagif Gasimov [12] proposed an improved version of Least Significant Bits (LSB) methodology. In the research work, two graphic files have been used and the algorithm is applied. One graphic file has been used as a container of information about the secret message and the other graphic file has been used as a steganographic key which is not transferred over the communication line, i.e., increasing its security against the attacker. Basic concepts of modern steganography and the applications of digital steganography in computer networking have been discussed.

3. Need of Research

The research has focused on the following:

1. To reduce the probability of data loss as the transmission has been made from multiple paths.
2. To improve the overall performance and security of the network using matrix splitter with the help of digital image processing.

3. To provide more secure and reliable mechanism to secure the graphical data due to transmission over the network. There would not be complete loss of data because information has been transferred from two different paths.

4. To maximize the security and minimize the limitation of traditional security techniques as proposed work would increase the security of a graphical matrix using an encryption mechanism after splitting digital information in two or multiple matrices.

5. To make appropriate use of parallel computing at the time of securing graphical contents because the graphical content is available in the form of a matrix. This matrix would be split using proposed mechanism.

6. To minimize time consumption. This time consumption would be reduced during the overall procedure of graphical image processing along with secure information transmission. Less time would be taken because all split matrices are transmitted in the same time instance on different paths.

4. Implementation and Results

4.1. Image Compression

Here the updated image compression algorithm has been used to compress an image. Here the JPEG image has been taken (as shown in Fig. 1) and MATLAB script has been applied to it.



Fig. 1: Original image

(A) Size of image after applying compression and decompression algorithm has been presented in Fig. 2 and Fig. 3.

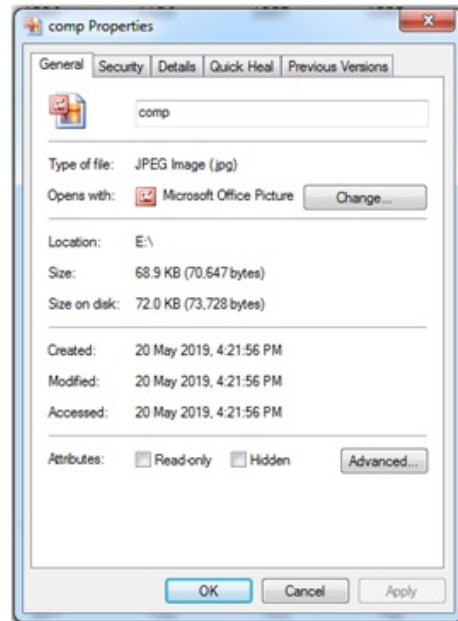


Fig. 2: Size of image after compression
(Elapsed time is 997.125608 seconds)

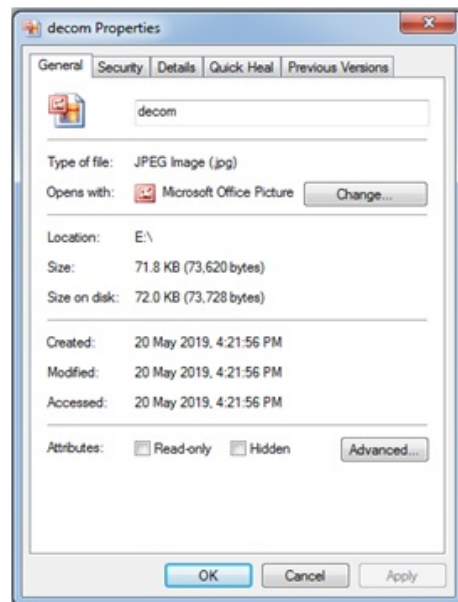


Fig. 3: Size of image after decompression
(Elapsed time is 0.128007 seconds)

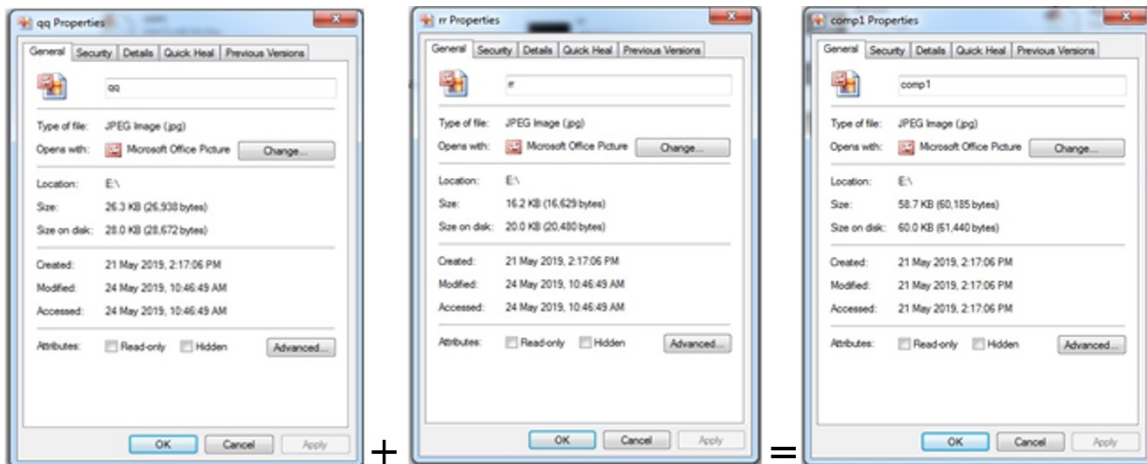


Fig. 4: Image Encoding using Splitter
 (Elapsed time is 1.024675 seconds)

(B) Proposed implementation has been made here. The Image Compression has been made using Graphical Bi-Matrix Splitter (see Fig. 4)

Here the original image has been split into two images and then combined to get a single image (as shown in Fig. 4). In this way the time taken to compress an image is much less as compared to the previously compressed image.

4.2. Matrix chart and the proposed work

Table 1 compares the various parameters of traditional and implemented work and found that the implemented work is better than the traditional work.

Some parameters like Comparison in Image Size, Time Consumption during compression, Mean

TABLE 1: Comparison of traditional and proposed (implemented) work via different parameters

Parameters	Traditional	Proposed work using Lossless Image Compression	Proposed work using Bi-Matrix Splitter	Proposed work using Quad-Matrix Splitter
Actual Size of File	135 KB	135 KB	135 KB	135 KB
Compressed size	68.9 KB	97.6 KB	58.7 KB	25.7 KB
Uncompressed Size	71.8 KB	53.8 KB	59.7 KB	26.8 KB
Mean square error	0.0063	0.00246 (average)	0.00263 (average)	0.00613 (average)
PSNR	70.2002	74.3182 (average)	73.9843 (average)	70.2902 (average)
Time consumption during compression	997.125608 seconds	15.457998 seconds	1.024675 seconds	0.736498 seconds
Extension of File	.jpg	.jpg	.jpg	.jpg

Square Error and PSNR (Peak Signal-to-noise ratio) values are evaluated (as shown in Table 1) on the basis of Original Image (Fig. 1). These results are plotted on some graphs (see Figures 5, 6, 7 & 8, respectively).

compression and proposed work using Bi-matrix splitter, i.e., only the split of graphical content into two matrices has been taken into consideration here while plotting graphs.

Note that all graphs are plotted on the basis of traditional work, proposed work using lossless image

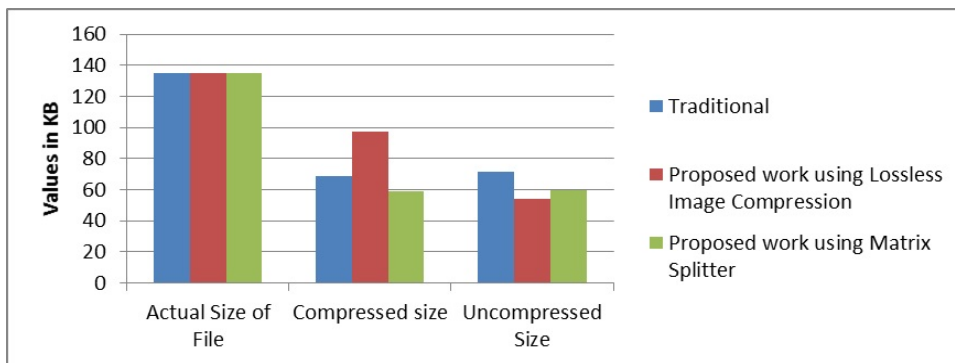


Fig. 5: Graph showing comparison in image size

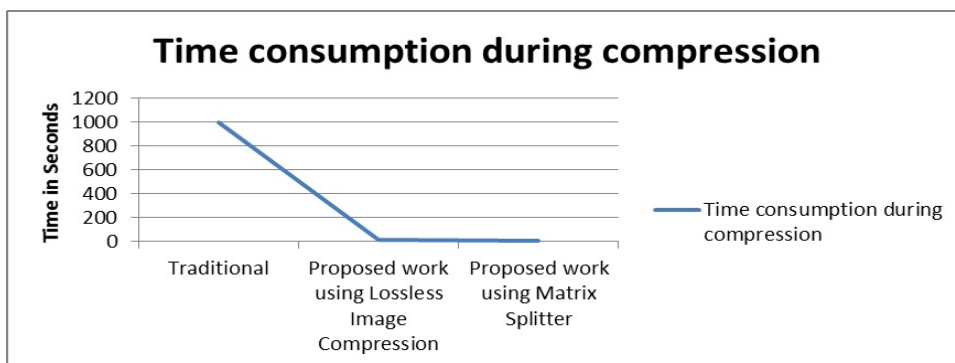


Fig. 6: Graph showing comparison of Time consumption during compression of images

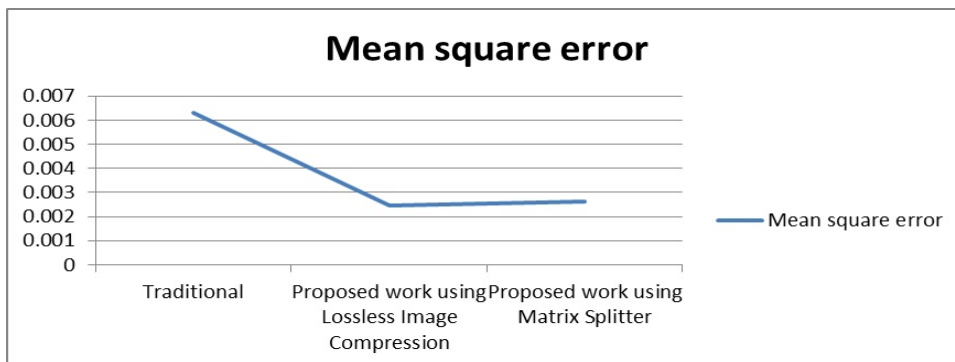


Fig. 7: Graph showing comparison of Mean Square Error of images

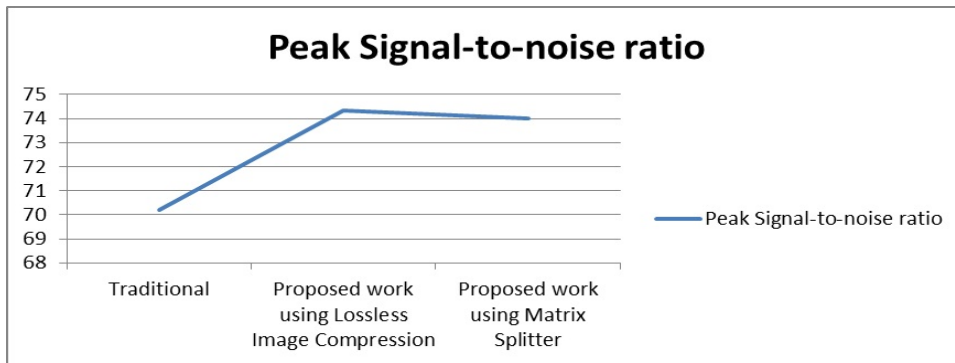


Fig. 8: Graph showing comparison of Peak Signal-to-noise ratio of images

4.3. Comparative Analysis of Packet Dropping in Traditional and Proposed Work:-

When data is transferred over the network, there is always a probability of attack and packet dropping. Here a comparison of packet dropping, in case of traditional and proposed work has been made (represented in Table 2).

TABLE 2: Comparison of Packet Dropping in Traditional and Proposed (Implemented) Work

No. of Packets sent	Packets dropped during Traditional work	Packets dropped during Proposed work
100	5	3
200	10	6
300	15	9
400	20	12
500	25	15
600	30	18
700	35	20
800	40	23
900	45	26
1000	50	29

The values depicted in Table 2 are also represented on the graph as shown in Fig. 9 below.

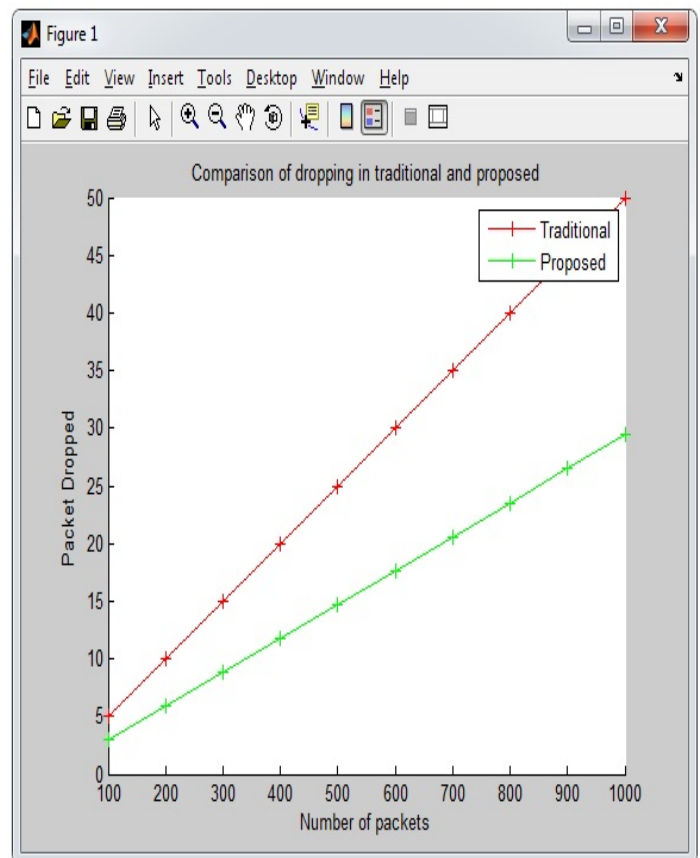


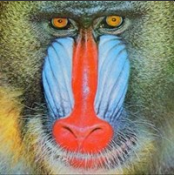


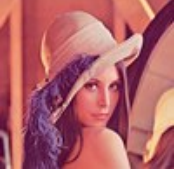
Fig. 9: Graph showing comparison of packet dropping in traditional and proposed (implemented) work

Here we can clearly see that the number of packets dropped is much less using proposed work (implemented) as compared to the traditional work.

The proposed implementation has also been made on some standard images (.jpg) using MATLAB. Here is the comparison between the compressed sizes using lossless image compression and graphical matrix splitter algorithms (given in Table 3) Here, both for the sender and the receiver ends, the results are displayed in two dimensions. At the sender end, one is Bi-matrix splitter, i.e., split of graphical content into two matrices and the other one Quad-matrix splitter, i.e., split of graphical content into four matrices. At receiver end, there is further merging of all these split matrices to get a single image, respectively, for each type of splitting. The results are displayed on the basis of the final result. Results in table 3 show that using the proposed technique with Graphical Matrix Splitter has much reduced the image sizes as compared to

the other algorithm. It also enhances the factor ‘time consumption’ as much less time will be taken for transmission of images because the split images also have much reduced sizes now as well and they will be transferred over different paths at the same time instance. Also, it is enhancing the network security of our graphical data over any network transmission medium because due to split images, if by chance, any third person attains one split image, it would be unable to be understood by that person due to lack of full information and it would be quite impossible for any person to track each and every path over which data is being transferred. So it is also increasing the network security of our data.

TABLE 3: Comparative analysis of Image sizes using traditional and proposed (implemented) algorithms

Figure	Name	Original Size	Image size with Lossless Image Compression	Image size with Graphical Bi-Matrix Splitter	Image size with Graphical Quad-Matrix Splitter
	Baboon	17.3 KB	9.3 KB	6.98 KB	2.11 KB
	Barbara	22.7 KB	7.39 KB	5.36 KB	2.51 KB
	Boat	35.5 KB	16.5 KB	11.8 KB	5.04 KB
	Lena	11.4 KB	2.57 KB	2.04 KB	1.01 KB

5. Encoding & Decoding done on Sender & Receiver Ends

5.1. Encipherment process with XOR operation

Encipherment: Steps included in enciphering data with XOR operation are as follows:

- Step 1:-** Get the data Y to encipher
- Step 2:-** For enciphering the data, take any randomly generated XOR key X
- Step 3:-** Perform XOR operation on data Y using key X i.e. $Z = Y \text{ XOR } X$, where Z is the output of the operation applied
- Step 4:-** Get the output Z as the enciphered data
- Step 5:-** Transmit the output Z as enciphered text over the network

Sample of enciphering algorithm:

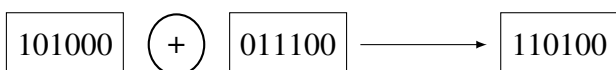
Suppose the original input data value (Y) for enciphering is 40 and randomly generated key (X) used to perform the XOR operation is 28

Binary value of 40 is 101000 (Y)
 Binary value of 28 is 011100 (X)

Perform $Z = Y \text{ XOR } X$
 $\Rightarrow Z = 40 \text{ XOR } 28$
 $\Rightarrow Z = 101000 \text{ XOR } 0111000$
 $\Rightarrow Z = 110100$

The enciphered data is 110100=52 (Z)

Output for Enciphering process using XOR



5.2. Decipherment process with XOR operation

Decipherment: Steps included in deciphering data with XOR operation are as follows:

- Step 1:-** Get the enciphered data Z to decipher
- Step 2:-** For deciphering the data, get the same randomly generated XOR key X used to encipher the data initially at Encoder side
- Step 3:-** Perform XOR operation on data Z using key X i.e. $Y = Z \text{ XOR } X$, where Y is the original data to be obtained
- Step 4:-** Get the data Y as the deciphered data
- Step 5:-** Use the deciphered data as the original required text where it is needed

Sample of deciphering algorithm:

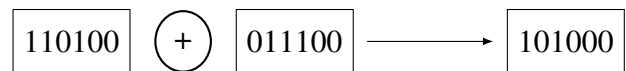
The input data for deciphering is 52 and the same XOR key X to perform XOR operation is 28

Binary value of 52 is 110100 (Z)
 Binary value of 28 is 011100 (X)

Perform $Y = Z \text{ XOR } X$
 $\Rightarrow Y = 52 \text{ XOR } 28$
 $\Rightarrow Y = 110100 \text{ XOR } 0111000$
 $\Rightarrow Y = 101000$

The deciphered data is 101000=40 (Y)

Output for Deciphering process using XOR



The same randomly generated XOR key X used for enciphering the data by the sender will be used for deciphering it by the receiver. The key will be revealed by the sender to the only receiver through a much secure channel or transmission medium. Since the data is enciphered, it will be unable for any intruder to understand it without deciphering it. As the key is randomly generated, it becomes

more difficult for the third person to guess and find out the key or to have any idea about it so easily. Without the key, the intruder will be unable to break the code. So it makes our data safe and more secure over any network transmission medium.

6. Conclusion

The proposed mechanism is more secure and reliable to secure the information present in the form of graphic. The security of data is provided at the time of transmission over the network. The present work is increasing the protection of data. It is capable to decrease the limitation of already present security techniques. This research is capable to overcome the time consumption at the time of graphical image processing with security of transmission. The proposed work has been utilized with the parallel computing while securing the graphical contents. To secure the content, the contents are split into two or multiple separate matrices. This research proved useful to reduce the probability of information loss at the time of transmission.

7. Future Scope

The research work would maximize the security and minimize the limitation of traditional security techniques. It would increase the security of a matrix using an encryption mechanism after splitting digital information in two, more than two or multiple matrices. The research work would also make appropriate use of parallel computing at the time of securing graphical contents. This matrix would be split using proposed mechanism. This research would opt to minimize chances of loss of data at the time of transmission as data is transmitted from multiple paths in the proposed work. The time consumption would be reduced during the overall procedure of graphical image processing along with

secure information transmission. It would improve the overall performance and security of the network using matrix splitter with the help of digital image processing. It would provide more secure and reliable mechanism to secure the graphical content.

Acknowledgments

The authors would like to thank to Assoc. Prof. Dr. Sedat Akleyek and the anonymous reviewers of the IJISS for their valuable comments, which have enhanced the quality of the paper.

References

- [1] T. J. Ogundele and A. O. Adetunmbi, "Evaluation of Multi Level System of Steganography", *International Journal of Information Security Science*, 3(4), December 2014.
- [2] I. Karadogan and R. Das, "An Examination on Information Hiding Tools for Steganography", *International Journal of Information Security Science*, 3(3), September 2014.
- [3] V. K. Pant, J. Prakash and A. Asthana, "Three step data security model for cloud computing based on RSA and steganography", *International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 490-494, Noida, India, 2015.
- [4] R. Kaur and J. Kaur, "Cloud computing security issues and its solution: A review," *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1198-1200, New Delhi, India, 2015.
- [5] F. Mary and D. I. G. Amalarethinam, "Data Security Enhancement in Public Cloud Storage Using Data Obfuscation and Steganography", *World Congress on Computing and Communication Technologies (WCCCT)*, pp. 181-184, Tiruchirappalli, India, 2017.
- [6] Ataussamad, R. Singh and S. Prakash, "Enhancement of steganography using K strange point clustering", *International Conference on Innovations in Information, Embedded and Communication Systems (ICIECS)*, pp. 1-5, Coimbatore, India, 2017.
- [7] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy and A. Ghoneim, "Secure Quantum Steganography Protocol for Fog Cloud Internet of Things", *in IEEE Access*, volume 6, pp. 10332-10340, 2018.
- [8] J. Zeng, S. Tan, G. Liu, B. Li and J. Huang, "WISERNet: Wider Separate-then-reunion Network for Steganalysis of Color Images," *IEEE Transactions on Information Forensics & Security*, Revised Version 2, p. 99, 2019.

- [9] Y. Yeung, W. Lu, I. Y. Xue, J. Huang and Y. Q. Shi, "Secure Binary Image Steganography with Distortion Measurement Based on Prediction", *IEEE Transactions on Circuits and Systems for Video Technology*, pp(99):1-1, 2019.
- [10] A. Y. AlKhamese, W. R. Shabana and I. M. Hanafy, "Data Security in Cloud Computing Using Steganography: A Review", *International Conference on Innovative Trends in Computer Engineering (ITCE)*, pp. 549 – 558, 2019.
- [11] A. Mukerjee, S. Som, S. K. Khatri and A. Mathur, "Enhancing Remembrance of Password as an Image", *Amity International Conference on Artificial Intelligence (AICAI)*, pp. 198 – 203, 2019.
- [12] V. Gasimov, "The Modified Method of the Least Significant Bits for Reliable Information Hiding in Graphic Files", *International Journal of Information Security Science*, 8(1), pp. 1-10, March 2019.