Information Security for Cloud using Image Steganography

Muhammad Amjad Khan¹, Taimoor Hassan², Zaka Ullah³

¹Department of Computer Science, Quaid-I-Azam University, Islamabad.

²National College of Business Administration and Economics (NCBA&E) Lahore.

³COMSATS University Wah, Pakistan
amjad97@gmail.com

ABSTRACT

Cloud computing is getting involved in almost every technological field to serve customers in a more efficient way. The shared resources (pool) with different configurations according to the user's needs are provided by cloud vendors. Users store their data on the cloud, data can be personal, or organizational, and data of every type must be secure on clouds. Making the data secure and reducing the integrity of data during transfer through public channels. In this paper, we will try to make data secure using image steganography. Using the steganography technique, we use encryption-decryption of data into images and make data invisible.

KEYWORDS: Cloud Computing, Steganography, K-Strange, Clustering Algorithm, Cryptography.

1. INTRODUCTION

Cloud Computing is helpful in day to day life. It is mainly being used for many apps/software by customers. The main properties of CC are scalability, service on demand, pooling, metered service & many more. National Institute of Standards and Technology (NIST) [1] defines cloud services used by customer customers can control and used in different manners:

- Software as a Service (SAAS)
- Platform as a service (PAAS)
- Infrastructure as a Service (IAAS)

In daily life cloud usage, storing data on the cloud, data can be personal or organizational. As usage increases massively, the ultimatum also increases. Most data can contain the virus for interruption due to the transfer of data using open channels. [2].

Many different methods are available for securing the data while transferring data hop to hop. Cryptography is most famous,

in this technique sensitive data is encrypted and then send, using some of the encryption algorithms or keys (key can be a phrase).

Steganography is the practice of concealing a message within another message or a physical object. It is a technique of hiding data using images as a cover. Any image can be used for steganography. Image format can be in the form of a bitmap, in png, etc. Hiding data in images can save the data for a very long time without being noticed. This method can use secure private

messages being transferred through the public network.[3].

Generally, it's possible to bind information(data) in images, but this technique requires digital media for securing data. Steganography can be done using different multimedia images like binary images, color images, grayscale images. The homogeneity in data and cover being used is not mandatory. This meant that audio can be embedded with the data or in the same manner data can be embedded with videos also.

Together steganographic and cryptographic methods are controlling and vigorous. In this paper, the main purpose is to evaluate numerous ways of joining steganography [12] and cryptographic methods to accomplish a cross-system. Moreover, some of the changes between cryptographic and steganographic methods were obtainable as well.

In this paper, we conduct a comparative study of steganography and cryptography. We review several approaches joining cryptography and steganography methods in one system. Moreover, we present an arrangement of these approaches, and comparison them in terms of the algorithm [13] used for encoding, the steganography technique and the file type used to cover the information.

2. RELATED WORK

Securing the digital medium (images) can be run by encrypting media-image. Encryption can be performed in a method that the actual image is reconstructed into the same appearance. Now, the main encryption algorithms or we can use such

algorithms that are suitable for working with images and pixels [4].

The encryption system which is described in the above section, plays' important role in containing key-generating and objects starting in the rule of cryptography. The running apps for such systems have been discouraged due to the pivot's fault [6].

The methods described in this paper are on a novel approach for hiding data in images. The 1st way is, to identifying of 2-bit code for information to be attached. The 2nd step is to use the image as a cover, hide the data using the selected cover using a 2-bit code. Then the data and image get combined and converted into bits [6].

The simple messages or text files can be embedded directly into the cover in the basic steganography technique. When the bits are to be inserted into the cover bits. Then at the end of the recovery, it tries to match the data bits in the bits of the pixel. If there are found any match between data bits and the pixel bits & the extreme nibble bits in the image, random pixels and process isn't hidden in any method. But if no matching found then this would be would result in's problem to store data [7].

3.PROPOSED METHODOLOGY

In this section we will describe the model of our work, in short, we can say that this will describe the working. We do implement the model we need a cover as an image, encrypted, decrypted, data to be hidden with the cover and after that actual secured image will be stored on the cloud.

Figure 1: Encrypt/Decrypt Data

Figure 2: Data Stored

This area gives the means associated with concealing the information. Typically, the useless code is produced as clarified in the accompanying section. As an underlying advance pick a spread picture, CI. Haphazardly elect the pixel (a, b) from CL here a & b signifies line and segment of picked

pixels individually. Give Aka a chance to speak to higher snack bit places of the pixel (a, b) i.e. Ak = 8, 7, 6, & 5. Give 'd' a chance for the information to be inserted and its period is meant by 'l' bits. Suppose that the nth piece is Dn.

The useless code is produced utilizes the accompanying advances.

1. Inspect the bit location Ak in Pixel (a, b), pixel is arbitrarily picked.
2. Check if an nth piece of information Dn is a matched bit location of Ak.
3. Distinguish code good for nothing i.e. 01, 00, 01 and 11 to be embedded along the coordinating location speaking to the extreme snack's bit locations.
4. Chances that the information bit doesn't coordinate, at that point bits in the higher snack are not quite the same as the information bit. suppose that there is a matching bit location 5 [8].
5. During translating the message, the beneficiary will be searched for this case. The beneficiary will find a supplement of the bit's in the 5th location which would be the information bit.
6. Rehash stage 1-4 will be information bit of Dn where $n < 1$ 2) Passcode base coordinating: Select a secret key 'Go' with 'CH' string length.

It can be of any length & could have any grouping of a string with capitalized or lowercased letter sets, & uncommon words. The secret phrase will be changed in the form of parallel code which would be utilized for putting away 1 bit for useless code.

Figure 3:Nibble Bits

The flowchart portrayed gives a pattern of exercises to be performed to insert information on the sender's side.

Figure 4: Insert Information

The flowchart portrayed gives a pattern of exercises to be performed to insert information on the sender's side.

Figure 5: Password Checking

4.PROPOSEDWORK IMPLEMENTATION

The proposed strategies work perfectly according to giving the privileged of the data or information covered up in a picture. So, information without much of a stretch is implanted into the spread picture and send using the public network to the collector. Speculation tests and examination demonstrates that this is a remarkable effect of techniques to be used for concealing information

according to the number of strings to be installed on spread picture. Consistently range for upcoming improvements for information privacy is a ceaseless problem in the present situation.

4.1. Improved K-Strange Clustering Algorithm:

Improved K-Strange Clustered Algo, improved K-Strange spike [10] shown in examination going to scan for the focuses which are max separated each other. Calculation likewise denotes impact according to the most distant focuses according to the informational collection. It finds the base K-minimum from the dataset & it's worth finding using calculation [11] in-between everyone according to the dataset. Besides, it's discovered maximum point from K-minimum. That figure is to be spoken K-maximum. Calculation upgrades chances by finding the 1st base point. By using that technique stays away from the choice of different focuses by calculation of the separation among focuses from the dataset. This acquires 0(nth) multifaceted nature periodically searching K-minimum & K-maximum. At that point, it will assess 3rd bizarre location inside the informational collection would be maximally isolated from focuses. On the other hand, there is some chance that the 3rd possibility is nearer to K-minimum, at that point location of the 3rd point is changed utilizing by choosing the in-between point next to 3rd distinct point & K-maximum & this last bizarre extraction. Be that as it may, if the third new point is nearer to K-maximum, at that point the situation of 3rd distinct point is moved by finding an in-between point [6].

4.2. Least Significant Bit Technique

It determined picture steganography epitomizes shrouded data at all critical bits of picture estimations to bearer picture. It divides the picture pixel to concealed information.

Table 1: Divide picture pixel

P1	10011111	01010100	10110101
P2	10000100	00010101	01010001
P3	11000100	11100111	01001011

The binary number 11111110 whose number is 254 is encapsulated into the LSB of the part of the image; and we obtain the data sets as shown below after encapsulating:

Table 2: Data sets after encapsulating

P1	10011111	01010100	10110101
P2	10000100	00010101	01010001
P3	11000100	11100111	01001011

Just 3 bits changed over as per the exemplified message. Yet, just not many bits in the picture will be adjusted to shroud mystery information. For

potential powers of every essential shading are 256, changing over the LSB of a pixel brings about a little believer in the forces of the hues.

Initially, actualizing K-Mean calculation & indicating a yield of both, sending end and recipient end individually. Presently working on similar tasks with Enhanced K-Strange.

Figure 6: A picture chooses for implementation

The optimized K-Strange Clustering Algorithm:

While expanding the size and higher dimensionality of information, Enhanced K-Strange Points Clustering Algorithm works superior to anything k-Means grouping. The table gives the immaculacy of the second strategy, which is a proportion of the level to which a group has things appropriate for the long bunch. Our proposed calculation runs quicker as well as gives great nature of bunches.

Table 3: Cluster algorithm values

Clustered Algo	Values
K-M	.81
Optimized	.84

Figure 7: Contribution for Enhanced K Strange technique

The bunches framed for the picture is as demonstrated as follows:

Figure 8: Information to be embedded

Adding information chunks in the image pixels. Appeared in the below fig:

Figure 9: Message addition into the biggest bunch

The information will be spread over 0-9 pieces on the image. With the information, its quantity is additionally added to the beneficiary through chosen media.

Figure 10: Stegoed picture at the receiver end

Information quantity is expected to provide just these strings characters of information. Trash esteem show, no information embedded in a specific location internally in pixels. The picture got on the beneficiary side is appeared in fig 10.

The bunches framed on the staged picture areas demonstrated as follows:

Figure 11: Output after optimized K-Strange Clustered method

At recipient nod staged picture is gotten & bunching is permeated & a similar procedure happens.

Correlation with the proposed system is: The groups shaped for the picture is as demonstrated as follows:

Figure 12: Final Cluster

Beginning along got yield in groups picks biggest 1 & addition's information similarly. As appeared below:

Figure 13: Matrix pixels output

5. RESULTANT

After the implementation and work, the following image was obtained by applying steganography using k-String min and max methods as discussed and implemented above. The image is shown in Figure13: contains the data that needs to be stored on the cloud showing as the image, but this image contains the hidden data

The following image is obtained after embedding the information using the k-strange method to image pixels. After applying the steganography, the image's actual pixels have not fluctuated. The picture is similar to before applying the steganography. The picture got in the beneficiary end is as demonstrated as follows:

Figure 14: Receiver side procedure - The staged picture.

The image received at the receiver's end will provide information as shown below after passing the image through decrypt or the information will be shown like below. The bunches framed on the staged picture are as demonstrated as follows:

Figure 15: Receiver side procedure: Output of K Means Clustering at beneficiary side alongside message evoked

6. CONCLUSION

In paper to acquire steganography, we have used K-Strange spikes Clustered Algo. In this paper, we have discussed steganography using different methods. In short, we are hiding the data by using an image as a cover. Cover images can be in any form bitmap, png, jpeg, etc. At that point we thought about the result of steganography strategies by using K-Mean grouping calculation, reason's that purposed technique of optimized K-Strange spikes Clustered Algo works perfectly as described.

REFERENCES

- [1] P. Mell and T. Grance, "NIST definition of cloud computing," National Institute of Standards and Technology, 2009.
- [2] P. Marwaha and P. Marwaha, "Visual Cryptographic Steganography in Images," in Proceedings of International Conference on Computing Communication and Networking Technologies, Karur, India, 2010.
- [3] W. Mazurczyk and K. Szczypiorski, "Is cloud computing steganographyproof?" 2011 Third International Conference on Multimedia Information Networking and Security, pp. 441–442, 2011.

- [4] X. Wang, J. Zhao, and H. Liu, "A New Image Encryption Algorithm Based on Chaos," *Optics Communications*, vol. 285, no. 5, pp. 562 – 566, 2012. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0030401811012430>
- [5] C. Zhu, "A Novel Image Encryption Scheme Based on Improved Hyperchaotic Sequences," *Optics Communications*, vol. 285, no. 1, pp. 29 – 37, 2012. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0030401811009540>
- [6] M. Amin, O. Faragallah, and A. Ahmed, "A Chaotic Block Cipher Algorithm for Image Cryptosystems," *Communications in Nonlinear Science and Numerical Simulations*, vol. 15, pp. 3484–3497, 2010.
- [7] A. Ahmed, X. Niu, and N. Wang, "Chaotic Image Encryption Using Bezier Curve in DCT Domain Scrambling," *Communications in Computer and Information Science*, vol. 194, pp. 30–41, 2011.
- [8] V. Patidar, N. Pareek, G. Purohit, and K. Sud, "A Robust and Secure Chaotic Standard Map based Pseudorandom Permutation-Substitution Scheme for Image Encryption," *Optics communications*, vol. 284, pp. 4331–4339, 2011.
- [9] W. Zhang, K.-w. Wong, H. Yu, and Z.-l. Zhu, "An Image Encryption Scheme Using Lightweight Bit-Level Confusion and Cascade Cross Circular Diffusion," in *Optics Communications*, vol. 285, 05 ,pp. 2343 – 2354, 2012.
- [10] Johnson, Terence, S.K. Singh, "Quantitative Performance Analysis for the Family of Enhanced Strange Points Clustering Algorithms", *International Journal of Applied Engineering Research*, Volume 11, Issue 9,, pp: 6872-6880, 2016.
- [11] Alfakih, Abdo Y, Henry Wolkowicz, and Amir Khandani, "Solving Euclidean distance matrix completion problems via semidefinite programming", *Computational optimization and applications*, Volume 12, Issue 1, pp: 13-30, 2015.
- [12] Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M., "Combination of steganography and cryptography: A short survey.", In *IOP conference series: materials science and engineering* (Vol. 518, No. 5, p. 052003), 2019.
- [13] Almuhammadi, S., & Al-Shaaby, A. "A survey on recent approaches combining cryptography and steganography. *Computer Science Information Technology (CS IT)*.", 2017.