Three State Baum Sweet Sequence with Steganography for Secured Cloud Data Storage and Access

M.Gomathe[1], S.Prasanna[2]
[1](Research Scholar, VISTAS)
[2](Associate Professor, VISTAS)

Abstract:- *In cloud environment, cloud user store information and accesses the same when required from the cloud server. Though several methods and mechanisms were introduced to address the security aspect, still full proof system related to security during data storage and access remains unsolved. In order to improve security during data storage and access, a novel steganography method, called, Mean Pixel Embedding based Image Steganography (MPE-IS) is designed. Three stages are involved in the design of MPE-IS. They are data preparation, embedding and extraction. In data preparation stage, gray scale image is considered as the cover image. The gray scale cover image is split into number of grids where each grid comprises two consecutive non-overlapping pixels represented in the form of matrix. The mean value between two consecutive non-overlapping pixels in the grid classifies the intensity of cover image, smaller mean value representing smoothened area and larger mean value representing the non-smoothened area. More cloud user bits are embedded into cover image in smooth area than in the non-smooth area. Next, an integrated Three State Baum Sweet Sequence technique is applied that performs embedding, and extraction as the inverse process. MPE-IS scans the gray scale image starting from the top to the bottom in a zigzag manner. The MPE-IS method hides the cloud user data into Baum–Sweet sequence for secured storage and data access. Here, the data is embedded inside the cover image to form stego-image. A Three-State Automaton (i.e. odd, even or zero) is employed during embedding. Whenever cloud user needs to access the embedded data from stego-image, Three-State Automaton (TSA) is used. By using the Three-State Automaton, cloud user data is retrieved from the cloud server in a secured manner. Experimental evaluation is carried out on factors such as data hiding capacity, PSNR, cloud data security and computational overhead with respect to varied number of cloud users and cover image sizes.*

Keywords:- *Baum sweet sequence, Hiding Capacity, Image Steganography, Mean Pixel Embedding, Three-state Automaton.*

I. Introduction

Digital image security plays a pivotal aspect in all areas. To name a few are, military, health center and so on. In the current years, one of the most popular services is the outsourced storage by cloud, especially for multimedia files, including images or videos that necessitates larger amount of storage. A new reversible method depending on Most Significant Bit (MSB) prediction was introduced in [1] with high capacity. In this reversible method, two approaches namely, High Capacity Reversible Data Hiding Approach with Correction of Prediction Errors (CPEHCRDH) and High Capacity Reversible Data Hiding approach with Embedded Prediction Errors (EPE-HCRDH) were investigated. A new Reversible Data Hiding in Encrypted Images (RDH-EI) method was introduced in [2] based on the Reversible Image Transformation (RIT). A reversible data hiding scheme depending on Shamir's secret sharing was introduced in [3] for ownership verification. The remainder of this paper is as follows. Through simplifications about related topics, methods and mechanism along with the issues related to handling of security using steganography techniques and analysis of related work are provided in Section 2. Section 3 describes the proposed methodology and algorithms. Section 4 demonstrates a proof of concept of the proposed method with the aid of parametric definitions, table and graphical representation, followed by a comparative analysis. Further conclusions are given in Section 5.

II. Related Works

Cloud computing has transformed the method of distributing computing services by providing software, infrastructure according to the needs consumer. Bio computing solution based on the polymerase chain reaction and primer generation was included in [5] to ensure confidentiality of data being sent. In [6], identity-based integrity auditing and data sharing was performed in [6] using sanitizer that sanitizes the data block corresponding to sensitive information therefore ensuring security and efficiency. To provide solution to this, user friendly visual cryptographic scheme was designed in [7] that in turn improved the visual quality of the recovered image and also meaningful shares. In [8], Encrypted Signals-based Reversible Data Hiding (ESRDH) technique was investigated using Paillier Encryption and value expansion, therefore ensuring embedding rate and average PSNR. To address this issue, a light weight encryption approach based on Layered Cellular Automata (LCA) was designed in [9] for protecting the privacy of sensitive data. Yet another privacy preservation mechanism was investigated in [10] based on the concept hierarchy and semantic relationships between concepts.

III. The problem definition

A cloud user intends to send a medical data to another cloud user or physician, via cloud. As, the medical data is sensitive, therefore, sending it without any embedding process is highly susceptible to several security risks. Hence, it is predominant to embed the cloud user medical data prior to transmission via cloud to ensure its privacy for secured data storage and access. To cope with this problem, Mean Pixel Embedding based Image Steganography (MPE-IS) is designed.

3.1 Methodology

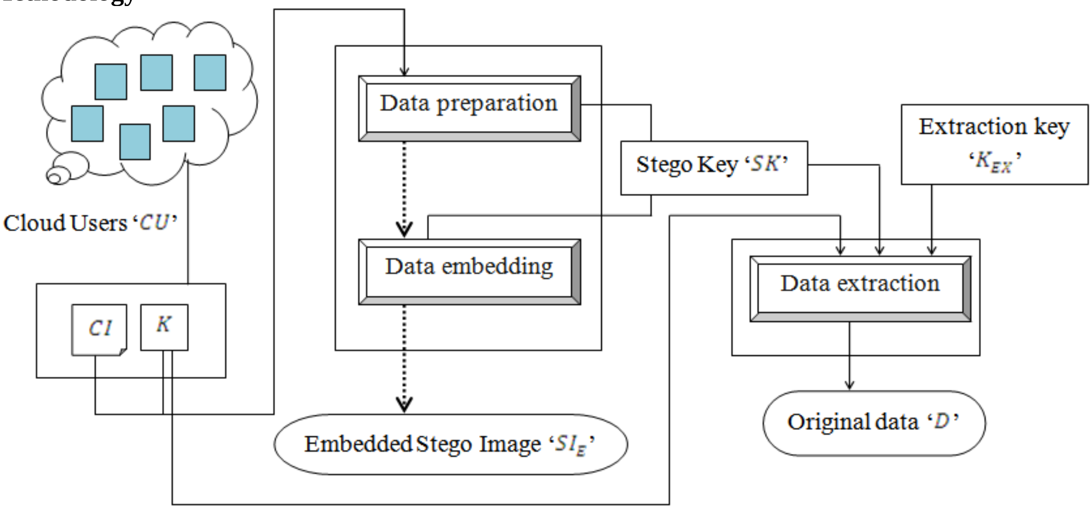


Figure 1 Mean Pixel Embedding based Image Steganography (MPE-IS)

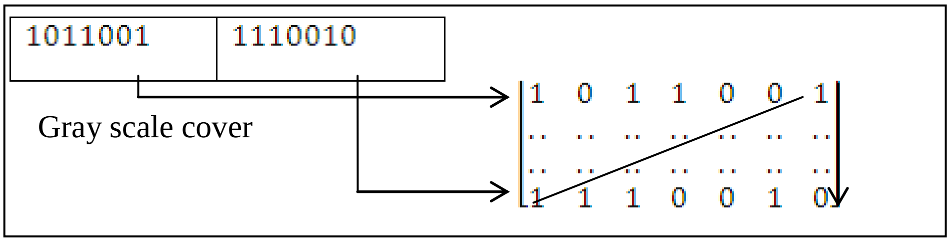
The proposed Mean Pixel Embedding based Image Steganography (MPE-IS) method addresses the problem of transmitting medical data in a secured manner to another concerned cloud user or physician. The MPE-IS method solves the mentioned problem using Cloud computing combined with steganography. The mechanism of the MPE-IS method is three-fold: 1) data preparation, 2) embedding, and 3) extraction.

As given in Fig 1, in data preparation stage, the non-overlapping pixels and mean pixel values are obtained using TSA-based steganographic scheme. In the second stage, the actual embedding process is carried on, with the stego key and cover image along with the secret data as input via cloud. Next, the stego image is forwarded to the cloud service provider. In the last stage, the concerned cloud user or the physician extracts the confidential data from the received stego image, therefore extracting the actual confidential data. This finally extracted data is then sent to concerned cloud users or physicians. The principal working of the MPE-IS method are explained in the sub-sequent sections.

3.2 Mean Pixel-based Data preparation technique

The data preparation stage comprises two fundamental operations including non-overlapping pixel representation and mean pixel value representation with transmission performed via cloud. The end-result of this stage is a stego image, containing important contents of the cloud user data. The first challenge is to identify the most important or confidential data (for example medical data).

Figure 2 Data Preparation



The gray scale cover image 'CI' is scanned from the top to the bottom in a zigzag manner. Let us consider two consecutive non-overlapping pixels 'p_i' and 'p_{i+1}', then, the mean value 'M_i' between two pixels are mathematically evaluated as given below.

$$M_i = \frac{(p_i + p_{i+1})}{2} \quad (1)$$

Next, the stego key is represented as the hexadecimal equivalent of 1st three Most Significant Bits. Then the data hiding key (i.e. stego key) is mathematically formulated as given below.

$$SK = HEX(K(1st\ 3MSB)) \quad (2)$$

Input: Cloud User '$CU = cu_1, cu_2, \ldots, cu_n$', Gray scale cover image '$CI = ci_1, ci_2, \ldots\ldots, ci_n$', Secret (i.e. Input key) 'K'

Output: Stego Key

```
Begin
    For each cloud user '$CU$'
        For each gray scale cover image '$CI$' with input key '$K$'
            Measure mean value between two pixels using equation (1)
            Obtain stego key '$SK$' using equation (2)
            Return (Stego Key '$SK$')
        End for
    End for
End
```

Algorithm 1 Mean Pixel-based Data Preparation

3.3 Integrated Three State Automaton Baum Secret Sequence Embedding technique

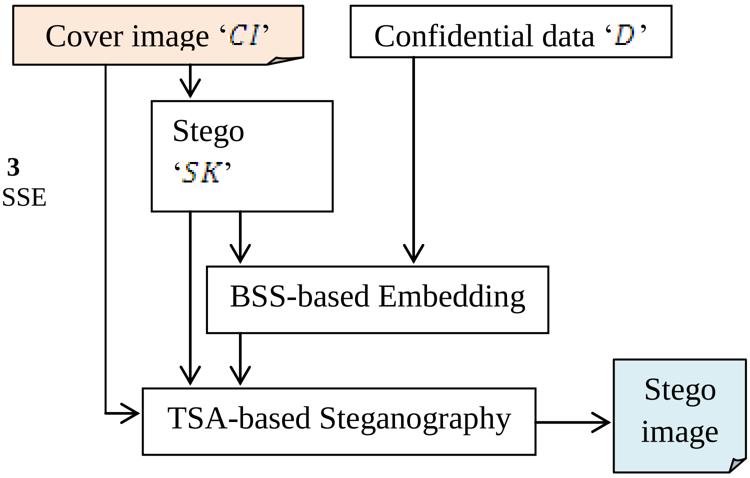


Figure 3
TSA-BSSE

As given in the Fig 3, for each cloud user 'CU' with the generated stego key 'SK' and confidential data 'D' and cover image 'CI' provided as input, BSS-based Embedding is performed, that includes two steps. Here, decimal equivalent of generated stego key 'SK' and confidential data 'D' is first acquired and stored as the resultant value '$ResValue$'. This is mathematically formulated as given below.

$$ResValue \rightarrow DEC(SK \cup D) \quad (3)$$

Then, with the equivalent resultant value '$ResValue$', BSS-based Embedding is formed. Next, the Baum Sweet Sequence is obtained. The Baum Sweet Sequence used in the MPE-IS work forms an infinite automatic sequence of '$0's$' and '$1's$' with two conditions. With the assumption of '$j \geq 0$', the two conditions are mathematically formulated as given below.

$$if\ (ResValue\ contains\ no\ consecutive\ 0s), BSS_j = 1 \quad (4)$$

$$if\ (ResValue\ contains\ cosecutive\ 0s), BSS_j = 0 \quad (5)$$

Then, the BSS-based embedding is represented as given below.

$$b_n = SK + D \quad (6)$$

$$b_n = \begin{cases} 1, if\ n = 0 \\ 0, if\ m\ is\ even \\ b_{\left(\frac{m-1}{2}\right)}, if\ m\ is\ odd \end{cases} \qquad (7)$$

From the above equation (7), if the value of '$n = 0$', then, the value of 'b_n' is '1'. On the other hand if the value of 'm' is even or odd, then the value of 'b_n' is said to be either '0' or '$b_{\left(\frac{m-1}{2}\right)}$'. Finally, by performing the TSA-based steganography, the resultant data 'b_n' stored in the gray scale cover image 'CI' forms the final stego image. (i.e., for example, the BSS for '$n = 32$', is '$1, 3, 4, 7, 9, 12, 15, 16, 19, 25, 28, 31$' from above equations (6) and (7) respectively). The pseudo code representation of Three State Baum Secret Sequence is given below.

```
Input: Cloud User '$CU = cu_1, cu_2, \dots, cu_n$', Gray scale cover image '$CI = ci_1, ci_2, \dots\dots, ci_n$', Data '$D = d_1, d_2, \dots\dots, d_n$', Stego Key '$SK$'
Output: Embedded Stego Image '$SI_E$'
Begin
    For each Cloud User '$CU$' with generated Stego Key '$SK$'
        For each gray scale cover image '$CI$' with Data '$D$' to be transmitted
            Obtain decimal equivalent of generated stego key '$SK$' and confidential data '$D$' using equation (3)
            Perform BSS-based embedding using equation (6) subject to constraints (4) and (5)
            Perform Three state automaton using equation (7)
            Return (Embedded Stego Image)
        End for
    End for
End
```

Algorithm 2 Three State Baum Secret Sequence Embedding

3.4 Integrated Three State Automaton Baum Secret Sequence Extraction technique

In this stage, the carefully encrypted medical image is disseminated i.e. sent to either another cloud user or physician via cloud. After getting the embedded stego image 'SI_E' from cloud, the cloud user requires the extraction of the hidden encrypted contents. Hence, an extraction algorithm is used to extract the required embedded data through steganography. Figure 4 shows the flow diagram of the extraction process.

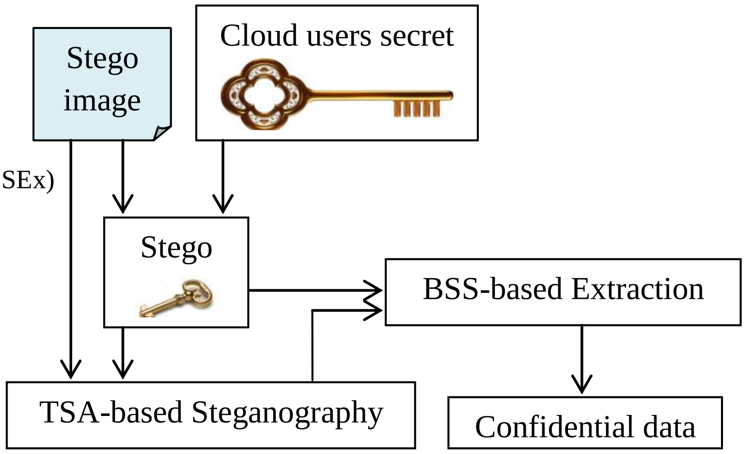


Figure 4 Three state Automaton Baum Secret Sequence Extraction (TSA-BSSEx)

```
Input: Cloud User '$CU = cu_1, cu_2, \dots, cu_n$', Stego Image '$SI = si_1, si_2, \dots, si_n$', Secret (i.e. Input key) '$K$', Stego Key '$SK$', Extraction key '$K_{EX}$'
Output: Confidential data
Begin
    For each Cloud User '$CU$' with Stego Image'$SI$', Secret (i.e. Input key) '$K$', Stego Key '$SK$' and extraction key '$K_{EX}$'  provided as input
```

```
            Perform BSS-based extraction using equation (8) resulting in the sequences
            Measure between values using equation (9) resulting in the non-sequences
            Obtain confidential data along using equation (10)
        End for
End
```

Algorithm 3 Three State Baum Secret Sequence Extraction (TS-BSSEx)

IV. Experimental evaluation

4.1 Hiding capacity analysis

In this section, the proposed method is evaluated from hiding capacity point of view. The hiding capacity in the proposed work is measured in terms of maximum hiding capacity. The maximum hiding capacity is the maximum amount of data that can be hidden in the gray scale cover image and is represented in the form of kilobytes. It is mathematically formulated as given below.

$$DHC = Size\ (D * CI) \qquad (11)$$

From the above equation (11), the hiding capacity 'HC' is measured on the basis of the size of the data 'D' (i.e. to be hidden) and the size of the cover image 'CI' respectively. It is measured in terms of kilo bytes (KB). The sample calculation is provided below followed by which, the table and graph representation are given.

Sample calculation

- **Proposed MPE-IS**: $HC = 10KB * 23.4KB = 234KB$
- **Existing Reversible Method**: $HC = 8KB * 23.4KB = 187.2KB$
- **Existing RDH-EI**: $HC = 7KB * 23.4KB = 163.8KB$

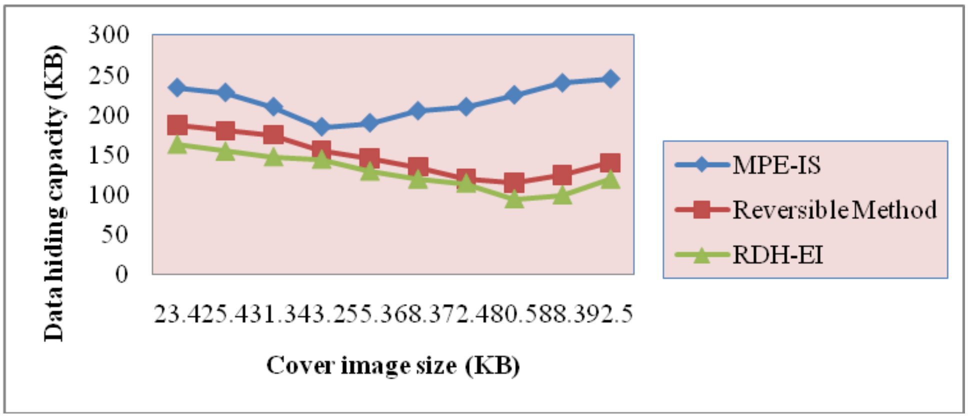


Figure 5 Comparative analysis using data hiding capacity

4.2 Distortion measurement analysis

In this section, the performance of various distortion measurements for sensitive data to be sent is analyzed. Two state-of-the-art image steganography methods are analyzed, including: Reversible Method [1] and RDH-EI [2] method.

$$MSE = \sqrt{\frac{1}{m*n}\sum_{i=i}^{m}\sum_{j=1}^{n}\left(O_{ij} - S_{ij}\right)^2} \qquad (12)$$

The distortion in the stego image is measured using the PSNR. The value of PSNR is obtained from [4]. In order to obtain lower distortion, higher PSNR value is desired. The value of PSNR is mathematically formulated as given below.

$$PSNR = 10 * \log 10\left(\frac{255 * 255}{MSE}\right) \qquad (13)$$

Sample calculation:

- **Proposed MPE-IS**: $PSNR = 10 * \log 10\left(\frac{255*255}{120}\right) = 37.33dB$
- **Existing Reversible Method**: $PSNR = 10 * \log 10\left(\frac{255*255}{160}\right) = 36.08dB$
- **Existing RDH-EI**: $PSNR = 10 * \log 10\left(\frac{255*255}{200}\right) = 35.12dB$

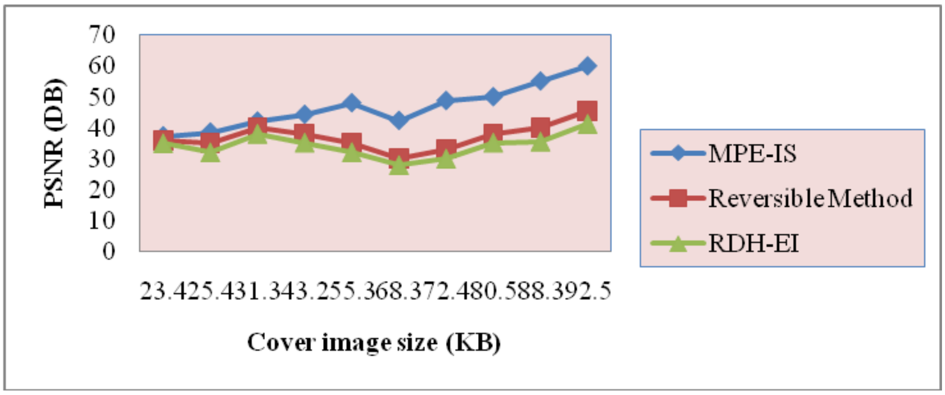


Figure 6 Comparative analysis using PSNR

V. Conclusion

Ensuring data storage/data access security using steganography techniques is considered a major challenge in cloud. This work proposed a high security method that combines the characteristics of binary number system and steganographic techniques. Decimal and hexadecimal number system is applied for data preparation to enhance the data hiding capacity. An integrated Three State Automaton Baum Secret Sequence Embedding (TSA-BSSE) is applied for embedding and extraction. With this, the noise ratio along with the computation overhead is said to be reduced, because of sequencing and non-sequencing of data present in image separately.

References

[1]. Pauline Puteaux and William Puech, "An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images", *IEEE Transactions on Information Forensics and Security, Vol. 13, Issue 7*, July 2018, Pages 1670 - 1681

[2]. Weiming Zhang, Hui Wang, Dongdong Hou and Nenghai Yu, "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation", *IEEE Transactions on Multimedia, Vol. 18, Issue 8*, August 2016, Pages 1469 – 1479

[3]. Priyanka Singh and Balasubramanian Raman, "Reversible data hiding based on Shamir's secret sharing for color images over cloud", *Information Sciences, Elsevier, Vol. 422*, 2018, Pages 77–97

[4]. G. Swain, S.K. Lenka, "Classification of spatial domain image steganography techniques: a study," *International Journal of Computer Science & Engineering Technology, Vol. 5, no.3*, pp.219-232, 2014

[5]. Sreeja Cherillath Sukumaran, Misbahuddin Mohammed, "PCR and Bio-signature for data confidentiality and integrity in mobile cloud computing", *Journal of King Saud University – Computer and Information Sciences, Elsevier*, Aug 2018

[6]. Wenting Shen, Jing Qin, Jia Yu , Rong Hao, and Jiankun Hu , "Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage", *IEEE Transactions on Information Forensics and Security, Vol. 14, No. 2*, Feb 2019

[7]. Pei-Ling Chiu, Kai-HuiLee, "User-friendly threshold visual cryptography with complementary cover images", *Signal Processing, Elsevier*, Oct 2014

[8]. Xianyi Chen , Haidong Zhong, Lizhi Xiong, and Zhihua Xia, "Improved Encrypted-Signals-Based Reversible Data Hiding Using Code Division Multiplexing and Value Expansion", *Security and Communication Networks, Hindawi*, Feb 2018

[9]. Xing Zhang, Seung-Hyun Seo, Changda Wang, "A Lightweight Encryption Method for Privacy Protection in Surveillance Videos", *IEEE Access*, Mar 2018

[10]. Zhangjie Fu Lili Xia Xingming Sun Alex X. Liu Guowu Xie, "Semantic-aware Searching over Encrypted Data for Cloud Computing", *IEEE Transactions on Information Forensics and Security, Vol. 13, Issue: 9,* Sept. 2018