IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Novel Scheme for the Watermarking in Cloud Computing

Gagandeep Kour[1], Yatin Agarwal[2]

M. Tech Student, Department of CSE, Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University, Lucknow, India[1]

Asst. Professor, Department of CSE, Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University, Lucknow, India[2]

ABSTRACT: The rapidly growing online services have paved the way for the emergence of a number of digital techniques. The contribution of these techniques is quite significant for preventing the illegal access, usage and alteration available on the social networking sites. The watermarking is one of the most commonly used techniques amongst all presented techniques. The watermarking techniques based on frequency domain make use of some inverting transformations such as DWT, DCT and DFT for image hosting. The frequency domain techniques merely vary the coefficient level of these transformations based on watermark and implement inverse transform to the real image for embedding watermark within the picture. But these techniques are extremely intricate and need more computing ability. In addition to this, these schemes offer greater repulsion against intrusions posing a security threat. An important approach in this category is GLCM.

KEYWORDS: DWT,DCT,GLCM, Watermarking, DFT

I.INTRODUCTION

Cloud computing is referred as a model that facilitates universal, suitable and on-demand network access for commonly used configurable computing resources having the ability of quick provisioning and releasing with minimum management effort from the client side and least service provider communication. Cloud computing is also regarded as the development of various technological advancements that work cooperatively for changing the approach an organization to construct their IT set-up[1]. Cloud computing does not make use of any new technology. In fact, all the technologies used by cloud computing are quite in practice. Cloud computing is an Internet-based computing approach. This approach includes both the applications provided as services in addition to the hardware and systems software in the framework that offer those amenities. In recent years, huge surge in the demand of these services, both commercially and educationally has been noticed [2]. Cloud computing is advantageous in different manners such as decreased cost, increased storage, higher rate of computerization and adaptability. All these factors have made cloud computing very popular among individuals, the public sectors, and commercial bodies [3]. An increased susceptibility to internal intrusions accompanies the economic and operational benefits of cloud computing. The cloud obfuscates the ID and position of mediators and the SPs (Service-Providers). It is possible to avoid confidentiality leaks effectively by intermediaries using Encryption but not at the end-points.In image processing, the images are processed generally in analogue and digital modes [4]. The first mode of analogue is used to generate the printed versions. These methods based on analogue approach provide basic understanding about images to users. The area of image processing is far beyond the image analysis. affiliation is one more essential task performed by visual schemes [5]. This is the reason that personal and collateral data is applied to the image processing. DIP (Digital image Processing) makes use of computers for the processing of digitized images. The data captured by satellites equipped with imaging capturing sensors lies in unstructured format. Therefore, it is required to apply different operations on this data to get useful information. the three universal operations that a wide range of data need to experience in DIP include pre-processing, enhancement, display, and knowledge retrieval.

There are huge facilities provided by the automated image analysis as well as knowledge acquisition systems that are dependent on the computer-driven processing images [6]. While analyzing the images as well as deriving knowledge from them, there are numerous issues to be resolved amongst which some are:

- It is evident to move away from the low-level pixel representation of the images. It is important to develop representation of images that can encode the contextual information hidden within an image which can be helpful in image mining process.
- The classification of gathered patterns is an important step within image mining process. An issue that is difficult to be resolved is the automatic derivation of appropriate decision criteria in order to perform clustering.
- Another major concern here is to propose an appropriate indexing mechanism. The procedures of indexing as well as extracting of knowledge from the images are important within these systems.
- The development and unification of the visual patterns and textual information from the query language is required.
- The image database that contains within it huge volume of images can be represented as World Wide Web. There is unlimited amount of information available behind the images. A major challenge within image mining and image processing is the analysis of web and retrieval of required knowledge from the images that are present online [7].

II.LITERATURE SURVEY

Shreyank N Gowda *et.al* [8] presented an enhanced dual layered encryption for approach based on the image steganography. In the Image steganography, the information was concealed and an image was employed as a medium. The LSB approach was one of the most conspicuous approaches for image steganography. The least considerable bit comprised in every pixel of an image was carried out for hiding the information in them. The limitation of this algorithm was that this algorithm was generated a simple for an attacker in concentrating the information from this algorithm. For this purpose, an algorithm was designed that assisted in maximizing the security of the algorithm. The entire data was taken in account in the presented approach for shaping one big block of information. In the initial phase, the AES algorithm was deployed for the encryption of information. After that, the RSA approach was carried out that had an additional layer for its security. The encrypted block of data was split into n blocks in which the client selected the n. Subsequently, the selection of n+1 images was done randomly and each block was hidden for which the LSB was employed with an image. The images were transmitted to random. However, the sequence was stored in a hash table that was hidden in the additional image. Every n+1 image was sent, the first "n" in a random request. The hash table was executed to extract the sequence. Then, the key was decrypted firstly and the entire data was decrypted later on.

Zaid Y. Al-Omari *et.al* [9] discussed that steganography was the science in which the secret messages were embedded inside other medium files due to which any stretch of the imagination hid the presence of the secret message. A novel steganography scheme was suggested for DIs that employed the RGB coloring model. The productivity of this scheme was tried and assessed. The outcomes revealed that stego images with high-quality which had resistibility against visual and statistical attacks. The pixel selection model was suggested for selecting the pixels which were qualified for Least Significant Bit modifications in adaptive manner on the basis of the threshold value in such a way that the pixels having color values amazingly dissimilar to their adjacent pixels were carried out initially and the pixels which had less difference were executed when they required on the basis of the size of the message.

Mamta Jain *et.al* [10] recommended a new strategy to transfer the medical information regarding patient securely within medical cover image for which the DT was carried out to conceal the data. The DT classifier provided a powerful method in which the decisions were provided to secret information that concealed the area within medical carrier image through the secret information mapping concept. The RSA approach had carried out to encipher the patient's one of a kind information. The structuring of result of the RSA was done ina variety of disseminated blocks in equal way. The mapping method that used breadth first hunt was implemented to allocate a secret cipher blocks to carrier image so that the data was inserted in steganography. The RSA decryption was deployed to obtain the hidden secret medical information regarding the patient by the beneficiary. Thus, only the authorized recipient was allowed to identify the plain text. Various parameters were carried out between medical stego and carrier images to break down and evaluate the execution. The outcomes were generated and their comparison was done with various existing algorithms.

Nikhil Simha H.N *et.al* [11] presented in this paper that security puts a critical part in correspondence applications to perform safe data exchanges. Image Steganographic process is a standout amongst the dependable procedure while encrypting and decrypting an image within other image in a unique manner that exclusive cover image was obvious. A frequency domain Image Steganography was presented in which Discrete Wavelet Transforms and Modified LSB least significant bit was utilized. The DWT was deployed to convert the spatial domain information into frequency domain

information. Image Steganographic procedure was further carried out using LL band. The inverse Least Significant Bit was implemented to decode the image. As the LL band was employed to encode and decode, the memory requirement of the design was less while executing the hardware. Similarly, the operating frequency of the architecture was maximized. A high PSNR was obtained for stegano and recovered hidden image using the recommended technique.

Shreyank N Gowda *et.al* [12] presented in this paper Steganography, a technique employed to hide any kind of information in which a few kind of cover medium was deployed. This information was available in different form. In the Image steganographic process, the used cover medium was a picture. The presented technique was a modulation of the standard LSB. The hidden information was considered as the text in this algorithm. This text was taken and the DES was executed with the assistance of a key initially for the encryption of this text. The RSA technique was deployed for the encryption of key that encrypted the data later on. The standard Least Significant Bit algorithm was applied to conceal the encrypted text. Subsequently, the image was forwarded. Initially, the RSA algorithm was carried out for decoding the key so that the data was unscramble. Then, this key was employed to extract the rest of the data with the help of decryption for which DES algorithm was deployed. A dual layer of security was obtained with encryption of text through DES initially. After that the RSA was used to encrypt the key for DES. The high reliability of the algorithm was guaranteed in this way.

SherinSugathan*et.al*[13] presented in this paper Steganography was the popular technique employed to hide the information which allowed the persons for the communication in secret way. The major benefit of this process was that the picture that encoded the secret had not considered by an attacker. The major objective of the techniques of image steganography dependably was to carry on the visual quality of an image when a secret message was encoded under it. The novel approach was presented to replace the image steganographic process based on the LSB for the RGB color images. An enhanced LSB embedding procedure was developed by exploring directional aspects of embedding data. The outcome demonstrated that the image quality was enhanced in terms of evaluation metrics PSNR and MSE. Various techniques were utilized for enhancing the quality of stegoimage. To achieve this, the secret data was embedded in the channels of least importance. The presented technique was integrated with those techniques yet it led to reduce the embedding capacity. Its implementation became easy in parallel hardware due to the data parallel scenario of the issue. The position of the direction bit can similarly be moved and the location was major aspect of a key to separate the secret data. A technique was carried out as a part of conjunction with encryption strategies for added security.

Aman Arora *et.al*[14] presented in this paper that the information was prepared for traveling around the world easily and economically as the technology and internet was developed speedily. The individuals suffered about their protection due to it. Steganography was a technique which prevented the unofficial users to approach the essential data. Several steganographic techniques employed by the users for hiding and mixing the information in other information because of which unauthorized users were unable to identify it. A diagram of Least Significant Bit strategy was provided in this paper. A unique algorithm was suggested and executed for the base steganography that was an enhanced and improved system in every aspect. The suggested technique was compared with the existing Least Significant Bit strategy on various parameters to obtain convincing and adequate results.

Shilpi Gupta *et.al*[15] presented in this paper that the internet and network applications were progressed rapidly in the most recent decade. This led to expand the episodes of digital attacks and traded off security. The communication was required to be reinforced and secured. The cryptography was established in this approach. Much work was done in this area but still advancement was required for tackling this problem. The asymmetric cryptography was considered and a new technique was suggested for which the two most prevalent algorithms named RSA and Diffie-Hellman were taken in account for accomplishing a greater security. At present, the suggested algorithm was proved valuable that had not various concept and ideas. Not only the effectiveness but the time complexity was revised to enhance the performance of the algorithm. The key size of encrypting and decrypting objective was mitigated further. The encryption and decryption were performed using the suggested algorithm. Moreover, this algorithm was carried for generation of digital signature.

A.H.M. Kamal *et.al* [16] presented in this paper that E-medicine was a procedure that provided health mind services to patients by the deployment of the Internet. A novel idea was suggested for modeling the e-medicine system's physical structure so that better disconnected health mind services were obtained. Smart cards were carried out for the authentication of the client in independent manner. Moreover, a unique process was recommended for verifying the identity of card owner and for embedding the secret data to the card when reports of persons who suffered from disease were provide at booths or at the e-medicine server system. The outcome obtained from simulation revealed that the suggested execution was validated

in authenticating the card and embedding methodology. To model the e-medicine system's physical structure was a unique suggestion. This system assisted in providing the medical service at the door of people. In addition, cure was provided in the distant villages from expert and specific city physicians in easy way due to which the health service got through the government of a nation was maximized. This system was proved beneficial for the people of every country.

Nikhil Patel *et.al* [17] proposed a mechanism for the space domain included in image steganography. The MSB of SI finished the modification of LSB of picture element related to CI. The dynamic key cryptography had provided the security as well as information hiding. The key was rotated to enable the dynamic component of key and a novel key was generated with each rotation of key. Based on the PRN that provided the double layer security to deal with the stegano analytic attack, the pixel of CI and secret image was selected under this strategy. The generation of three sets of pseudo noise sequences was carried out for hiding the MSB of each pixel of the secret image through the Least Significant Bit of all the pixels of the CI under this process. A key vector of size having 192 bits pseudo noise sequences was produced and efficient security was offered to execute this algorithm.

III.RESEARCH METHODOLOGY

With the rapid growth of internet the various digital methods has been proposed to protect the multimedia information from the non-authorized accesses use and change. Among all the proposed methods the watermarking technique is the most common technique for protecting the multimedia data for unauthorized access. The water marking methods have been categorized as spatial domain method and frequency domain method. In spatial domain method we modify the lower order bits of cover image to embed the water mark. This work is based on the image watermarking in which original image can be hiding under the watermark image and it will be the final watermarked image. This technique increases the security of the images by using various type of encoding schemes. When the encoding schemes are applied to generate the final watermarked image, the properties of the original image need to be analyzed and these properties are color and textural properties. The properties of the image can be analyzed by using DCT and DWT algorithms. These algorithms are based on wavelet transformation techniques for image processing. The encoding schemes which can be applied are RSA and Diffie-helman. These two algorithms are used to establish secure channel from source to destination and data which is watermarked data is transmitted through secure channels. In this work, RSA and Diffie-helman algorithm are compared in terms of security in image watermarking .The proposed algorithm consists of following steps :-

1. **Pre-processing phase**: - The pre-processing the first phase of the proposed algorithm. In this phase the size of the input and watermark image will be made size for the efficient watermarking

2. **Apply DCT, DWT and SVD algorithm for watermarking: -** In the second phase, the DCT and DWT and SVD algorithm are applied which will generate the watermarked image. The detail description of these algorithms is given:-

i. Discrete Cosine Transform (DCT): In DCT based strategy insertion of secret information in bearer depends on the DCT coefficients. Any DCT coefficient value above legitimate threshold is a potential place for insertion of secret information. Here the Most Significant Bits of secret image are hidden in Least Significant bits of just those pixels of cover image whose DCT coefficient value is more prominent than a specific threshold value. The Discrete Cosine Transform (DCT) transforms the image from spatial domain to frequency domain. It separates the image into spectral sub-bands with respect to its visual quality, i.e. high, middle and low frequency components. DCT is a mechanism to transform successive 88-pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain. The least significant bits of the quantized DCT coefficients are utilized as redundant bits into which the hidden message is embedded. The modification of a single DCT coefficient affects each of the 64 image pixels. Since this modification happens in the frequency domain and not the spatial domain, there are no observable visual differences. The advantage DCT has over different transforms is the capacity to minimize the square like appearance resulting when the boundaries between the 8x8 sub-images get to be visible (known as blocking artifact) [18].

ii. Discrete Wavelet Transform (DWT): Any wavelet transform for which the wavelets are discretely test are called discrete wavelet transform (DWT). The key advantage DWT has more than Fourier transforms is worldly resolution. A 2-dimensional Haar DWT consists of two operations: One is the horizontal operation and the other is the vertical one. At to start with, scan the pixels from left to ideal in horizontal heading. At that point, play out the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the privilege. Repeat these operations until

every one of the rows are processed. The pixel sums speak to the low frequency part denoted as image L while the pixel differences speak to the high frequency part of the original image denoted as image H. Furthermore; scan the pixels from top to bottom in vertical heading. Play out the addition and subtraction operations on neighboring pixels and afterward store the sum on the top and the difference on the bottom. Repeat this operation until every one of the columns is processed. At long last we will get 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and subsequently looks fundamentally the same as the original image [19].

iii. Singular Value Decomposition (SVD): The singular value decomposition (SVD), one of the most useful tools of linear algebra, is a factorization and approximation technique which effectively reduces any matrix into a smaller invertible and square matrix [20]. One special features of SVD is that it can be performed on any real m n × matrix. It factors A into three matrices U, S, V, such that

$$A = USV^T$$

Where, U and V are orthogonal matrices and S is a diagonal matrix.

This diagonal matrix is responsible for an image luminance and orthogonal matrices are responsible for the geometry of an image. In this algorithm, the authors found the singular values of cover image and then modified them by adding a watermark. SVD transform is again applied on the resultant matrix for finding the modified singular values. These singular values are combined with the known orthogonal components to get the watermarked image. For watermark extraction, inverse process is used.

3. **Analyze robustness' of the watermarked image**: - In this phase, the watermarked image is analyzed by implementing salt & pepper, contrast and sharpen attack on the watermarked image.

4. **Apply Secure channel establishment algorithm: -** In the fourth phase, the algorithm of secure channel establishment is implemented which will establish secure channel from source to destination. In this step proposed algorithm is analyzed under two algorithms. The first algorithm is RSA algorithm and second algorithmisdiffie-helman algorithm. These two algorithms are used to establish secure channel from source to destination. This provides extra security to the watermarked image at time of transmission. The detail description of these algorithms is given below:-

5. Extract of Watermarking: - The watermarked image will be received at the destination and if the key which is generated gets matched with the entered key then the extract process takes place. To extract the original image from the watermarked image inverse SVD, inverse DWT and inverse DCT will be applied in the proposed algorithm.

IV.RESULT AND DISCUSSSION

The quantitative analysis is the type of analysis which can represent the visualization change in the image. To analyze the results the existing and proposed algorithms are implemented on the certain images.

The qualitative comparison is the in which the values of the algorithms are compared in terms of PSNR, MSE etc. The algorithms are diffie-helman, Base paper algorithm and RSA algorithms.

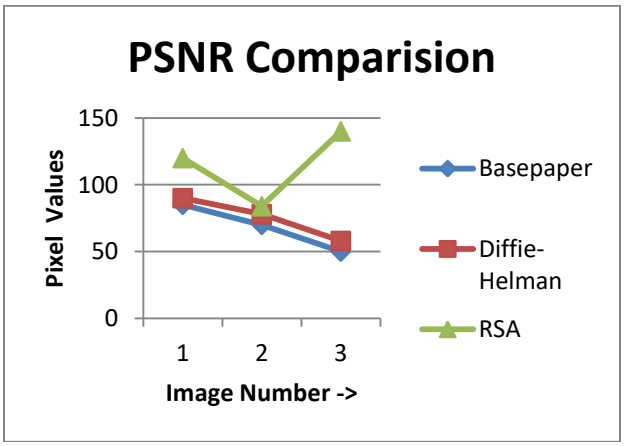

Fig 1: PSNR Comparison

As shown in figure 1, the comparison of proposed and existing algorithm is done in terms of PSNR. The algorithm which has maximum PNSR value is more reliable as compared to algorithm which has minimum PSNR value.

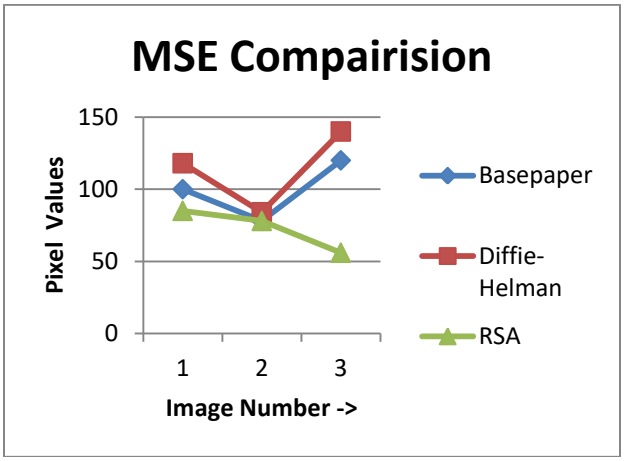

Fig 2: MSE comparison

As shown in the figure 2, the MSE of the proposed and existing algorithm is compared and it is been analyzed that algorithm which has high MSE value less reliable than the algorithm which has less MSE value.

V.CONCLUSION

The watermarking is the efficient technique which provides security to the original image. In this work, it is been concluded that to watermarked image is generated using DCT, DWT and SVD algorithms. To analyze the robustness of the watermarked image various attacks are implemented and these attacks are contrast, salt & pepper and sharpen attack. The differ-helman algorithm is applied which will establish secure channel from source to destination. The performance of diffie-helman algorithm is compared with the RSA. It is been analyzed that performance of diffie-helman is matter than RSA in term of PSNR, MSE and SSIM.

REFERENCES

[1] Robert Crone and Soo-Choon Kang, "Image Processing Techniques for Analysis of Air Bearing Surfaces", Vol. 38, No. 1, IEEE TRANSACTIONS ON MAGNETICS, 2002.
[2]Chenn-Jung Huang, Chi-Feng Wu, Chua-Chin Wang, "Image Processing Techniques for Wafer Defect Cluster Identification", IEEE, pp 0740-7475, 2002.
[3] A.S. Bahaj and P.A.B. James, "CHARACTERISATION OF MAGNETOTACTIC BACTERIA USING IMAGE PROCESSING TECHNIQUES", 1993, IEEE TRANSACTIONS ON MAGNETICS, Vol. 29, No. 6.
[4] Yun Cao, Xianfeng Zhao, and Dengguo Feng," Video Steganalysis Exploiting Motion Vector Reversion-Based Features", IEEE SIGNAL PROCESSING LETTERS, VOL. 19, NO. 1, 2012.
[5] Yun Cao, Hong Zhang, Xianfeng Zhao and Haibo Yu," Covert Communication by Compressed Videos Exploiting the Uncertainty of Motion Estimation", 2013, IEEE, 1089-7798
[6]Qiang Cheng and Thomas S. Huang," An Additive Approach to Transform-Domain Information Hiding and Optimum Detection Structure", 2001, IEEE TRANSACTIONS ON MULTIMEDIA, Vol. 3, No. 3
[7]SorinaDumitrescu, and Xiaolin Wu," A New Framework of LSB Steganalysis of Digital Media", 2005, IEEE TRANSACTIONS ON SIGNAL PROCESSING, Vol. 53, No. 10
[8]Shreyank N Gowda, "Advanced Dual Layered Encryption for Block Based Approach to Image Steganography", 2016, International Conference on Computing, Analytics and Security Trends (CAST)
[9] Zaid Y. Al-Omari, Ahmad T. Al-Taani, "Secure LSB Steganography for Colored Images Using Character-Color Mapping", 2017 8th International Conference on Information and Communication Systems (ICICS)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

[10]Mamta Jain, Rishabh Charan Choudhary, Anil Kumar, "Secure Medical Image Steganography with RSA Cryptography using Decision Tree", 2016, IEEE
[11] Nikhil Simha H.N., Pradeep M. Prakash, Suraj S. Kashyap, Sayantam Sarkar, "FPGA Implementation of Image Steganography using Haar DWT and Modified LSB Techniques", 2016 IEEE International Conference on Advances in Computer Applications (ICACA)
[12]Shreyank N Gowda, "Dual Layered Secure Algorithm for Image Steganography", 2016, IEEE
[13]SherinSugathan, "An Improved LSB Embedding Technique for Image Steganography", 2016, IEEE
[14] Aman Arora, Manish pratap Singh, Prateek Thakral, Naveen Jarwal, "Image Steganography using Enhanced LSB Substitution Technique", 2016, IEEE
[15] Shilpi Gupta and Jaya Sharma, "A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman", 2012, IEEE
[16] A.H.M. Kamal, M. Mahfuzul Islam, "Facilitating and securing offline e-medicine service through image steganography", 2014, Healthcare Technology Letters, Vol 1, Iss 2, pp. 74–79
[17] Nikhil Patel, Shweta Meena, "LSB Based Image Steganography Using Dynamic Key Cryptography", 2016, IEEE

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details