IJERMT

International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

January-February-2019 Volume 6, Issue-1

Email: editor@ijermt.org www.ijermt.org

TECHNIQUE OF WATERMARKING IN CLOUD COMPUTING ENVIRONMENT TO IMPROVE SECURITY OF DATA WITH GLCM ALGORITHM

Dr. Vikas Jain,

Assistant Professor, SCRIET-DCA,

Ch. Charan Singh University, Meerut, Uttar Pradesh, India

Abstract

Cloud computing is a concept that is still in the process of developing. It offers consumers a data outsourcing service that is free of disputes, which frees them from the burden of maintaining their own data storage management. On the other hand, giving priority to the establishment of a trustworthy and secure data archive in the face of doubtful service providers need to be the major focus. Using the PCA and GLCM algorithms to extract features from the source picture and to generate a semi-blind watermarked image, the primary emphasis of this study is on the use of watermarking technology for the purpose of copyright protection in cloud computing. The use of digital watermarking to cloud computing has the potential to significantly improve the system's security and make user data more protected.

Keywords: *Cloud computing, watermarking, GLCM algorithm*

INTRODUCTION

Through the act of embedding certain data into the medium, digital watermarking is a method that transforms data that has been input by the user into an integral component of digital media. This method has a wide range of applications, some of which include information authentication, data indexing, database monitoring, and broadcast monitoring. Other applications include monitoring broadcasts. In order for a digital watermarking system to achieve optimal performance, it must be able to strike a compromise between the competing goals of perceptual transparency, data capacity, and resistance against assaults. In order to investigate these tradeoffs, we use a viewpoint that is founded on information theory. Two primary applications for watermarks are as follows: When it is regarded a transmission code, a watermark is classified as belonging to the first category. In this case, the decoder is responsible for accurately retrieving all of the data that has been sent. The watermark is used as a code of authentication for the second batch of documents. One and only one of the functions of the watermark detector in the second system is to determine whether or not a certain pattern is present.

Individuals have the ability to include verification messages or copyright notices into digital audio, video, or picture signals and documents via the use of digital watermarking. Documents that are stored digitally may likewise be safeguarded using this way. The concealed message that is now being discussed is comprised of bits that reveal information about the signal or the person who created it (such as their name, location, or other relevant information). Watermarking is a security measure that may be applied to paper or cash, and the technology gets its name from this security measure. Despite the fact that digital watermarking does not possess the steganographic quality of being invisible by the naked eye, there are watermarking technologies that possess this quality. Steganography is a technique for concealing data that includes concealing information inside a message in such a manner that the receiver does not detect it.

During the early 1990s, the Internet saw a tremendous amount of success, which brought to light the financial opportunities that might be derived from the delivery of multimedia content via online networks. A confirmation of this promise was provided by the advent of the World Wide Web. As a result of the fact that company executives are enthusiastic about using digital networks for

Their principal reasons for wanting to maintain the protection of their ownership rights are to ensure that they may continue to produce digital content for the purpose of generating financial advantage. In order to do this, some people have suggested using digital watermarking. The digital signals or patterns that are included into digital photographs are known as digital watermarks. Because this signal or pattern is present in each and every duplicate of the original, digital watermarks have the potential to serve as digital signatures for copies of an image that have not been changed throughout the process. There are two types of watermarks: one kind may be shared by several copies (for example, to indicate who generated the document), and another type can be unique to each copy (for example, to identify who got the document). Regardless of the circumstances, the original document must be converted into a different format in order to ensure that the watermark is properly applied. The most important distinction between digital watermarking and digital fingerprinting is that the latter includes the creation of a new file that "describes" the contents of the former file while the original file remains unaffected. This is the essential difference between the two. For instance, the checksum field of a disk sector is a straightforward illustration of this concept since it functions as a fingerprint of the data block that came before it. Hash algorithms are also used to build fingerprint files, which is somewhat similar to the previous example.

DIGITAL WATERWARKING TECHNIQUES

Based on various kinds of reports present, the computerized watermarking procedures are arranged into different classifications. They are:

1.Content watermarking: Through the use of this technology, the content archive is safeguarded against violation of copyright requirements. There were three different types of advanced watermarking that were demonstrated, and they are as follows:

Line move coding is one approach that may be used for the purpose of encoding archives. This method involves vertically changing the region of content lines.

Codes that make use of word movement: Flat-moving the word area is one method that may be used to encode the record. Programming for the highlights: At this point, he selects and modifies certain highlights that are included inside his strategy.

2. Picture Watermarking: Utilizing this technique, the watermark is included into the photos. It is not a simple undertaking to remove the watermark since it is already an intrinsic component of the picture because it is already there.

3. Video Watermarking: The provision of this cryptographic data is accomplished by the use of cryptographic data that is derived from computer video frames. During this phase, the client can only decrypt the encrypted data that is contained in certain films. This is only possible with a considerable deal of effort. The process occurs between the first, plain, and checked videos.

4. Sound Watermarking: Through the use of this technique, an electronic identity is included into the sound wave. The media files that were used in the audio recording are organized in a way that makes it possible to recover the information via the utilization of a variety of installation solutions.

Purpose of digital watermarking

The usage of invisible watermarks, on the other hand, might be helpful in determining who published, developed, owned, distributed, or authorized the use of a document or picture. It is possible to do this via the use of watermarks. To achieve this particular objective, we want to identify the images in a way that cannot be undone and that eliminates any possibility of disagreement over who is credited with what or what is assigned to them. The watermark would make it much easy to demonstrate ownership, collect copyright earnings, or penalize the offender in the case that the content was used without permission. In addition, watermarking has been suggested as a method for verifying the authenticity of photographs in the case that they are distributed without permission. Books that were protected by copyright were often restricted in the past because it was impossible to replicate and distribute them in large quantities. On the other hand, with the assistance of contemporary digital networks, the dissemination of knowledge on a huge scale is now simple and inexpensive. Through the use of digital watermarking, it is feasible to brand each photo in a way that is unique to each individual purchaser. In the case that the buyer goes on to create a copy, it is possible to present persuasive evidence of the illegal duplicate that occurred.

OBJECTIVE

1. one, to learn about cloud computing watermarking
2. In order to analyze the safety of data stored in the cloud

METHODOLOGY

The use of watermarking is an efficient way for securing the data related to pictures. There are two primary categories that watermarking techniques fall into, and those are blind and semi-blind watermarking methods. The following are the key objectives of the technique that has been suggested:

1. For the purpose of producing semi-blind watermarks, it is proposed that the DVT technique be improved.
2. The GLCM algorithm will serve as the foundation for the proposed method, which will be used to evaluate the characteristics of the original picture.
3. the strategy that was recommended into action and investigate how well it performs in comparison to the current state of the art in terms of MSSIM, BER, and PSNR.

The steps of the recommended technique include embedding, extraction, and disassembling the cover image. These stages are included in the framework. The watermark that is implanted will present itself as a binary watermark image. In order to investigate the textual characteristics of the picture, we make use of the DWT approach in combination with the GLCM methodology. This method is great for creating sets for blind watermarks due to the fact that it is straightforward in its implementation.

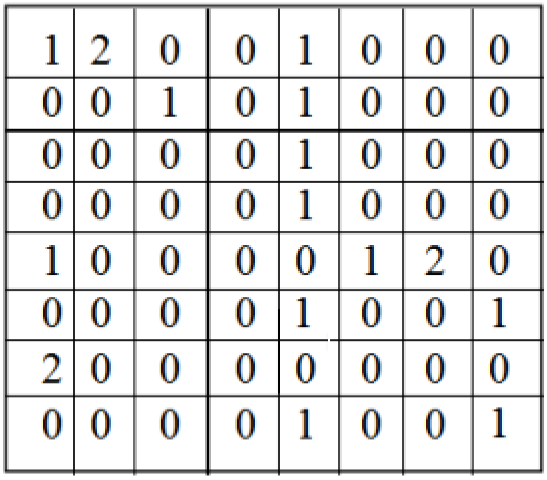
Gray-level co-occurrence matrix (glcm):

Through the use of the gray level co-occurrence matrix that was constructed in this article, statistical texture characteristics may be discovered. There are many different texture features that may be extracted with the help of the GLCM. In statistical texture analysis, the construction of texture characteristics is accomplished by making use of the statistical distribution of the observed combination of intensities at specified sites in relation to each other in the image. On the basis of the amount of intensity points (pixels) that are present in each combination, statistics are differentiated into three distinct orders: first order, second order, and higher order. Making use of the GLCM is one method that may be used to extract second-order statistical properties of the texture. textures of a third or higher level take into consideration the connections that exist between three or more pixels in the structure of the image. Although it is theoretically possible, the difficulties of computing time and interpretation preclude it from being successfully implemented on a mass scale.

The GLCM of an image is a table that provides a listing of the frequency with which certain luminance values are found in pixels. In the GLCM, the position of pixels that have grayscale values that are similar to one another is kept. The GLCM compute units receive pairs of gray level data via the input process. A0b1, a2b3, a10b21, and other combinations of gray values are some examples of the potential gray value combinations that may be employed in the GLCM calculating unit. This is where we can observe the difference between the photo that was originally taken and the one that was forecasted.

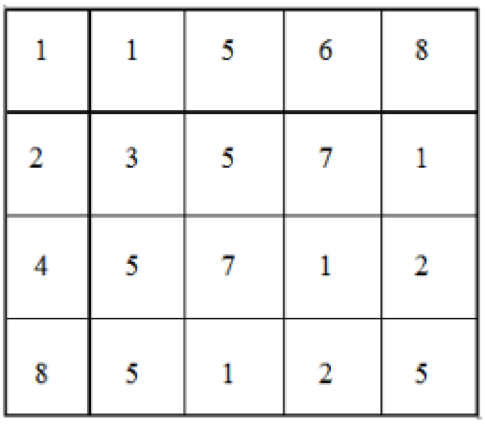
Taking into consideration the relationship between two nearby pixels, the GLCM takes into account the fact that the first pixel is referred to as a reference pixel and the second pixel is referred to as a neighbor pixel. Within the GLCM, the number of gray levels in the image is denoted by the symbol Ng, and the matrix is square in shape with Ng dimensions. One of the elements of the matrix is used to indicate the occurrence of each pair of pixels that have values i and j.A co-occurrence matrix is a matrix in which each row and column comprises a group of possible image values. Consider, for instance, the 4x5 matrix that is shown in figure I.

Equivalent GLCM matrix for the above image I is



1	2	0	0	1	0	0	0
0	0	1	0	1	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	1	0	0	0
1	0	0	0	0	1	2	0
0	0	0	0	1	0	0	1
2	0	0	0	0	0	0	0
0	0	0	0	1	0	0	1

fig : GLCM Image Matrix



1	1	5	6	8
2	3	5	7	1
4	5	7	1	2
8	5	1	2	5

fig: Image Matrix

There are a number of statistics that can be derived from the GLCMs using the matlab function once they have been created. Some information on the texture of a picture may be obtained from these statistics. There are fourteen textural features that are assessed from the probability matrix in order to extract the characteristics of texture statistics of remote sensing images, as stated by the co-occurrence matrix. Below are some of the characteristics listed.

1. Uniformity or energy is another name for the angular second moment. A measure of picture homogeneity, it is the sum of squares of the GLCM angular second moment entries. When the picture has excellent homogeneity or when the pixels are highly comparable, it's high.
2. It is the local homogeneity that represents the inverse difference moment (IDM). When both the local gray level and the inverse GLCM are high, it is high.
3. It reveals how much picture data is required for the compression process. The entropy of a transmitted signal is a measure of the information or message loss as well as the picture information.
4. This metric assesses the linear relationship between the gray levels of adjacent pixels.

The Proposed Algorithm Can Applied in Following Steps:

1. Kindly include the grayscale cover photo that is 512 by 512 pixels.
2. In order to get a 32x32 matrix with LL4 coefficients, you need use DWT at level 4.
3. I created a vector user interface with dimensions of 1024 by 128 pixels using the photo that I had gotten.
4. In order to construct a set with dimensions of 1024 by 2, we may now dispute about the magnitude of the Vi vector in relation to its quantization vector V.
5. Generate an output that is 1024 by 1.
6. It is necessary to first quantify the image data in order to obtain the pixels before you can proceed with the generation of a GLCM square matrix of dimensions NxN.
7. To normalize the GLCM, divide the total number of elements by each element (i, j) in the matrix. This will bring the GLCM to its normalized state. After that, the components that were produced are utilized as probabilities in order to find the connection and extract the texture characteristic.
8. The eighth step is to make use of the principal component analysis (PCA) method in order to dynamically select the scaling factor R from the characteristics that were retrieved in step 7. 9. Insert the watermarking picture (yi) into the cover image by utilizing the following equation, taking into consideration the expected output from step 5 and the R value from step 8.

$$Ui = Zi + \alpha * Yi$$

9. It is possible to make a final, semi-blind image that is watermarked..

RESULT ANALYSIS

Within the scope of this section, we demonstrate the effectiveness of four distinct techniques. A portion of the MATLAB simulation is dedicated to the investigation of image robustness and PSNR. By using this method, a lot of photographs that have a wide variety of pixel types are processed. The PSNR, MSE, BER, and MSSIM scores are the metrics that we use to evaluate the quality of the watermarked photographs.

PSNR: An examination of the peak-to-signal ratio is one method that may be used to ascertain the degree of visibility that both the watermarked and extracted watermark photographs possess. It is defined by the mean squared error that represents the difference between the pixel values of the watermarked picture and the pixel values that correspond to the cover image. It is standard practice to make use of this function because of the clarity and simplicity it has. When the PSNR number is higher, it suggests that the reconstructed image may be considered of better quality.

MSE: The total squared difference between the original and compressed pictures is what the mean square error (MSE) measures. It is a measure of the entire squared difference. A lesser number of MSE implies that the error was made less often.

BER: Bit Error Rate : This is the definition of the BERT, which stands for the number of errors in bits per second. When calculating the bit error rate (BER), the total number of bits that are transferred during a certain period of time is divided by the number of bit errors that occur during that time period.

MSSIM: SSIM, which stands for Multi Scale Structural Similarity Index Measurement, is a perceptual metric that assesses the degree to which processing procedures, such as data compression, negatively impact the quality of pictures. It is a method for assessing the degree to which two photographs are comparable to one another. The technique that was first created by SSIM is expanded upon by MS-SSIM, which builds upon it by doing several SSIM picture evaluations at varied image sizes.

In order to accomplish this effect, each succeeding image pair is subjected to a down sampling factor that is two times larger than the previous one. This process is repeated several times.

Performance analysis

	Parameter values	Leena	Taj	Cat	Rcert
WATERMARK IMAGE	PSNR	24.40	27.36	24.70	25.17
	MSE	238.16	120.39	221.88	199.27
CONTRAST ATTACK	PSNR	24.80	27.80	25.16	25.06
	MSE	239.19	108.78	199.73	204.47

SHARPEND ATTACK	PSNR	19.82	25.78	24.52	14.69
	MSE	683.63	173.30	231.53	226.58
SALT & PEPPER ATTACK	PSNR	30.06	31.34	30.28	30.31
	MSE	64.65	48.16	61.43	61.01

Following is the analysis of values when we applied our proposed methodology :

	Parameter values	Leena	Taj	Cat	Rcert
WATERMARK IMAGE	BER	0.07	0.08	0.09	0.05
	MSSIM	160.08	64.09	90.69	224.09
CONTRAST ATTACK	BER	0.00	0.18	0.06	0.06
	MSSIM	255.00	133.70	239.52	233.65
SHARPEND ATTACK	BER	0.02	0.08	0.07	0.21
	MSSIM	253.81	125.80	231.96	219.69
SALT & PEPPER ATTACK	BER	0.01	0.9	0.03	0.04
	MSSIM	254.57	157.54	234.56	232.72

The Proposed algorithm is implemented in MATLAB by considering the authentic dataset.

CONCLUSION

In spite of the increasingly broad use of cloud computing, cloud security continues to be a serious problem. Within the context of cloud security, this paper proposes a watermarking-based strategy to manage trust between data owners and service providers. The purpose of this study is to throw new light on cloud security. A conclusion that can be drawn from this article is that watermarking is an efficient approach for hiding sensitive information that is encoded in images. The operating capability-based watermarking strategy has been improved in this instance by using the GLCM and PCA algorithms together. The PCA algorithm is responsible for selecting the retrieved image features, while the GLCM technique is responsible for extracting the features of the original picture. Based on the results of the simulation, we have determined that the strategy that was recommended is effective in terms of both PSNR and MSE. Over the course of the future, we want to conduct further cloud computing experiments in order to assess the effectiveness of our approach, which has the potential to become a benchmark for cloud security.

References

1. U. Yadav, J.P. Sharma, D. Sharma and P.K. Sharma, "Different Watermarking Techniques and its Applications: A Review", International Journal of Scintilla and Engineering Research, Vol. 5, no.4, (2014)April.

2. Chih-Chin Lai and Cheng-Chih Tsai, "Digital Image Watermarking Using Discrete Wavelet Transformand Singular Value Decomposition", IEEE TRANSACTIONS ON INSTRU-MENTATION AND MEASUREMENT, VOL.59, NO.11, NOVEMBER 2010.

3. C.-c. Lai and c.-c. Tsai, "Digital Image Watermarking Using Discrete Wavelet Trans-form and Singular Value Decomposition", IEEE Transactions on Instrumentation and Measurement, vol. 59, no.11,(2010) November.

4. M. Narang and S. Vashisth, "Digital Watermarking using Discrete Wavelet Transform" International Journal of Computer Applications (1975-88887) vol.74, no.20, (2013)July.

5. Salama, A., Atta, R. , Rizk, R. Wanes, F., "A robust digital image watermarking technique based on wavelet transform". In: IEEE Int. Conf. on Sys. Eng. and Tech., pp. 100-104 (2011).

6. Ahmed S. Salama, Mohammed A. AI- Qodah, Abdullah M. Tliyasu, Awad Kh. AI-Asmari and Fei Yan: A Hybrid Fusion Technique for watermarking Digital Images: Advances in Intelligent Systems and ComputingVolume240, pp 207-217,(2014).

7. lliyasu, A., Le, P., Dong, F., Hirota, K.: Watermarking and authentication of quantum images based on restricted geometric transformations. Information Sciences 186(1), 126-149 (2012). 562.

8. AI-Asmari, A., Salama, A., T1liyasu,A., AI-Qodah, M.:ADWT ordering scheme for hiding data in images using pixel value difference. In: IEEE Eighth Int. Conf. on Computational Intelligence and Security(CIS), pp. 553-557 (2012).

9. Abid Khan, Ayyaz Yaqoob, Kinza Sarwar, Mouzna Tahir, Mansoor Ahmed, "Secure Logging as a Service Using Reversible Watermarking", The 12th International Conference on Future Networks and Communications, (FNC-2017)

10. Rita Choudhary, Girish Parmar, "A Robust image Watermarking Technique using 2-level Discrete Wavelet Transform (DWT) ", IEEE 2nd International Conference on Communication, Control and Intelligent Systems(CCIS)

11. Mr. Y. Gangadhar, Dr. V.S.Giridhar Akula, Dr. P. Chenna Reddy, " A Survey on Geo metric Invariant Watermarking Techniques" ,2016 IEEE

12. Ahmed S. Salama, Mohamed Amr Mokhtar, "Combined Technique for Improving Digital Image Watermarking", 2016 2nd IEEE International Conference on Computer and Communications

13. Mr. R. D. Shelke, Dr. Milind U. Nemade, "Audio Watermarking Technique Protection : A Review", 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication

14. Chengxiang Yin, Jin Hu, Xuejun Zhang, Xiang Xie, "Advertising system based on cloud computing and audio watermarking", 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing

15. Muhammad Imran and Bruce A. Harvey, Adnan Ali Memon, "A Novel Blind Color Image Watermarking Technique Based on Singular Value Decomposition and Principal Component Analysis", 2016, The Sixth International Conference on Innovative Computing Technology

16. U. Yadav, J.P. Sharma, D. Sharma and P.K. Sharma, "Different Watermarking Techniques and its Applications: A Review", International Journal of Scintilla and Engineering Research, Vol. 5, no.4, (2014)April.

17. Chih-Chin Laiand Cheng-Chih Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL.59, NO.11, NOVEMBER 2010.

18. C.-c. Lai and c.-c. Tsai, "Digital Image Watermarking Using Discrete Wavelet Trans- form and Singular Value Decomposition", IEEE Transactions on Instrumentation and Measurement, vol. 59, no.11, (2010) November.

19. M. Narang and S. Vashisth, "Digital Watermarking using Discrete Wavelet Transform" International Journal of Computer Applications (1975-88887) vol.74, no.20, (2013)July.

20. Salama, A., Atta, R. , Rizk, R. Wanes, F., "A robust digital image watermarking technique based on wavelet transform". In: IEEE Int. Conf. on Sys. Eng. and Tech., pp. 100-104 (2011).