Novel Technique to Increase Cloud Data Security

Pratul Sharma
Deptt. Of Computer Science & Engineering
Dr. Brajesh Kumar Singh
Head, Deptt. Of Computer Science & Engineering
R.B.S Engineering Technical Campus, Bichpuri, Agra

Abstract:

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. A novel method is proposed which deals with secure extraction of data by utilizing transform based image watermarking techniques. The conventional transforms are applied in an optimized mode in these schemes in different spatial regions of the image to embed a watermark. The scheme is subjected to Signal processing attacks and Geometric attack to test against the robustness of the image. The watermarking of image is made secure by testing against unauthorized detection techniques employed by attackers. This is realized by a correlation based detector applied to the scheme. Experimental results show that the watermarked image is robust and secure against Signal Processing attacks, Geometric attacks and unauthorized Detection attacks.

Keywords: Watermarking, Cloud Computing, Security

Introduction:

Digital watermarking is a process in which some information is embedded within a digital media so that the inserted data becomes part of the media. This technique serves a number of purposes such as broadcast monitoring, data authentication, data indexing and so forth. A digital watermarking system must successfully satisfy trade-offs between conflicting requirements of perceptual transparency, data capacity and robustness against attacks. These trade-offs are investigated from an information-theoretic perspective [1]. Watermarks have two categories of roles: In the first category, the watermark is considered as a transmission code and the decoder must recover the whole transmitted information correctly. In the second category, the watermark serves as a verification code. In the latter system, the watermark detector must simply determine the presence of a specific pattern. Since the footprint of the verification watermarking, that is, the number of pixels per watermark code bit is typically higher, this case has higher robustness as compared to the subliminal channel (transmission code) case. In watermarking schemes, the watermark message is embedded in the host signal in different ways, for example, additively or multiplicatively. For about ten years, several reversible watermarking schemes have been proposed for protecting images of sensitive content, like medical or military images, for which any modification may impact their interpretation [2]. These methods allow the user to restore exactly the original image from its watermarked version by removing the watermark. Thus it becomes possible to update the watermark content, as for example security attributes (e.g., one digital signature or some authenticity codes), at any time without adding new image distortions. However, if the reversibility property relaxes constraints of invisibility, it may also introduce discontinuity in data protection. In fact, the image is not protected once the watermark is removed [3]. So, even though watermark removal is possible, its imperceptibility has to be guaranteed as most applications have a high interest in keeping the watermark in the image as long as possible, taking advantage of the continuous protection watermarking offers in the storage, transmission and also processing of the information. Digital Watermarking software looks for noise in digital media and replaces it with useful information. A digital media file is nothing more than a large list of 0's and 1's. The watermarking

software determines which of these 0's and 1's correspond to redundant or irrelevant details [4]. For example, the software might identify details in an image that are too fine for the human eye to see and flag the corresponding 0's and 1's as irrelevant noise. Later the flagged 0's and 1's can be replaced by a digital watermark. The SVD is the optimal matrix decomposition in a least square sense that it packs the maximum signal energy into as few coefficients as possible. Singular value decomposition (SVD) is a stable and effective method to split the system into a set of linearly independent components, each of them bearing own energy contribution. Singular value decomposition (SVD) is a numerical technique used to diagonalizable matrices in numerical analysis [5]. SVD is an attractive algebraic transform for image processing, because of its endless advantages, such as maximum energy packing which is usually used in compression ability to manipulate the image in base of two distinctive subspaces data and noise subspaces, which is usually uses in noise filtering and also was utilized in watermarking applications. Each of these applications exploits key properties of the SVD. The discrete wavelet transform (DWT) is a linear transformation that operates on a data vector whose length is an integer power of two, transforming it into a numerically different vector of the same length. It is a tool that separates data into different frequency components, and then studies each component with resolution matched to its scale. DWT is computed with a cascade of filtering followed by a factor 2 sub sampling [6]. A neural network is defined as "...a computing system made up of a number of simple, highly interconnected processing elements, which process information by their dynamic state response to external inputs." The idea of ANNs is based on the belief that working of human brain by making the right connections can be imitated using silicon and wires as living neurons and dendrites.

Literature Review:

Ali Al-Haj, (2007) described about the proliferation of digitized media due to the rapid growth of networked multimedia systems, has created an urgent need for copyright enforcement technologies that can protect copyright ownership of multimedia objects [7]. In this paper, they describe an imperceptible and a robust combined DWT-DCT digital image watermarking algorithm. The algorithm watermarks a given digital image using a combination of the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform(DCT). Performance evaluation results show that combining the two transforms improved the performance of the watermarking algorithms that are based solely on the DWT transform.

Surya Pratap Singh, (2012) presents [8] a robust watermarking technique for color and grayscale image. The proposed method involves many techniques to conform a secure and robust watermarking. In the proposed technique the watermark is embedded in 3rd level of DWT (Discrete Wavelet Transform) and before embedding the watermark image is passed through chaotic encryption process for its security, other important thing is that in the proposed method watermark is embedded in the form of DCT (Discrete Cosine Transform) with special coefficient shifting algorithm to minimize the impact on main image. The performance of the proposed watermarking is robust to a variety of image processing techniques, such as JPEG compression, enhancement, resizing, and geometric operations.

A Mansouri et.al (2009) a new robust method of non-blind image watermarking is proposed [9]. A new non-blind SVD-based watermarking method in CWT domain was introduced. Modifying SVs of the host image in CWT domain provides high robustness against the common attacks. High PSNR of watermarked image is another beneficial point of the algorithm as the result of CWT implementation. Making tradeoff between PSNR of the watermarked image and correlation between extracted watermark and the original data lead to selecting the best value of the scaling factor in both variant and non-variant implementations of

our method. The additional privilege of suggested algorithm is its compatibility with human visual system characteristics to embed the watermark by selecting the best sub-bands in CWT domain. In this way, high capacity of CWT domain is applied to embed the watermark information along with preserving the quality of the watermarked image**.**

Anthony T.S. Ho et.al (2011) In this paper, they propose [10] a robust image-in-image watermarking algorithm based on the fast Hadamard transform (FHT) for the copyright protection of digital images. To increase the invisibility of the watermark, a visual model based on original image characteristics, such as edges and textures are incorporated to determine the watermarking strength factor. To further increase the reliability of the watermarking against the common geometric distortions, such as rotation and scaling, a post-processing technique is proposed. The performance of the proposed algorithm is evaluated using Stirmark. The experiment uses container image of size 512×512×8bits and the watermark image of size 64×64×8bits. It survives about 60% of all Stirmark attacks. The simplicity of Hadamard transform offers a significant advantage in shorter processing time and ease of hardware implementation than the commonly used DCT and DWT techniques.

Alexander Sverdlov et.al (2003) proposed [11] both Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) have been used as mathematical tools for embedding data into an image. In the DCT-domain, the DCT coefficients are modified by the elements of a pseudo-random sequence of real values. In the SVD domain, a common approach is to modify the singular values bythe singular values of a visual watermark. In this paper, we present a new robust hybrid watermarking schemes based on DCT and SVD. The singular values in each quadrant are then modified by the singular values of the DCT-transformed visual watermark. We show that embedding data in lowest frequencies is resistant to one set of attacks while embedding data in highest frequencies is resistant to another set of attacks. The only exception is the rotation attack for which the data embedded in middle frequencies survive better.

Fang Li, (2009) In this paper, they proposed [12] a two-stage method for demising images heavily contaminated by salt and pepper noise. In the first stage, we use adaptive median filter to detect the noisy pixels. All the pixels are marked as noisy or noise-free pixels. In the second stage, we take the noisy pixels as inpainting regions and noise-free pixels as true information. The inpainting task is done by the normalized mean curvature flow. The method is generalized to color image. Experimental results show that the proposed algorithm has advantages over nonlinear filtering or regularizing methods in terms of edge preservation and noise removal and is competitive with other two-stage methods in the literature.

Research Methodology:

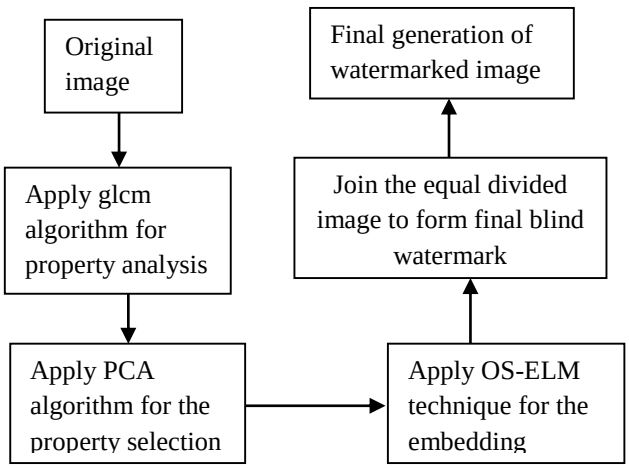

Fig 1: Proposed Flowchart of embedding

The watermarking is the efficient technique to provide security to the image data. The watermarking techniques are broadly classified into blind and semi-blind watermarking techniques. In the base paper, the semi-blind watermarked image is generated using the OS-ELM technique which the machine learning technique. The four levels DWT technique is applied to extract the features of the original and watermark images. The training images which are analyzed with the DWT algorithm is given as input to generate final training sets for the generation of semi-blind watermarks. The DWT algorithm will analyze textual features of the images which can be replaced with the GLCM algorithm which has less complexity and easy to generate training sets for the generation of blind watermarks.

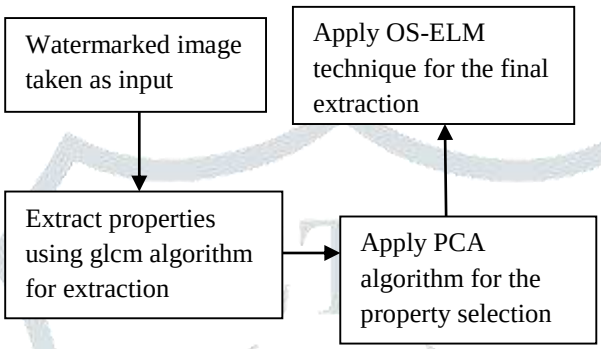

Fig 2: Proposed Flowchart for extraction

Experimental Results:

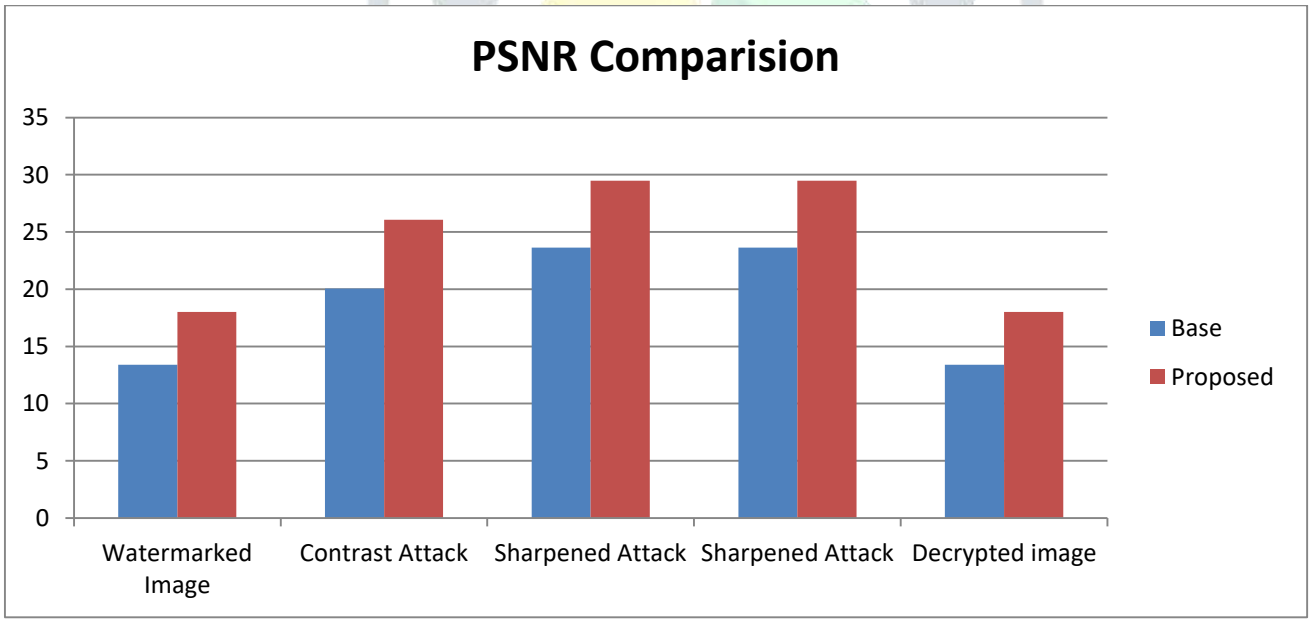

Fig 3: PSNR Comparison

As shown in figure 3, the PSNR value of the watermarking image, salt & pepper, sharpen, decrypted is compared It is analyzed that decentralized image has maximum PSNR value.

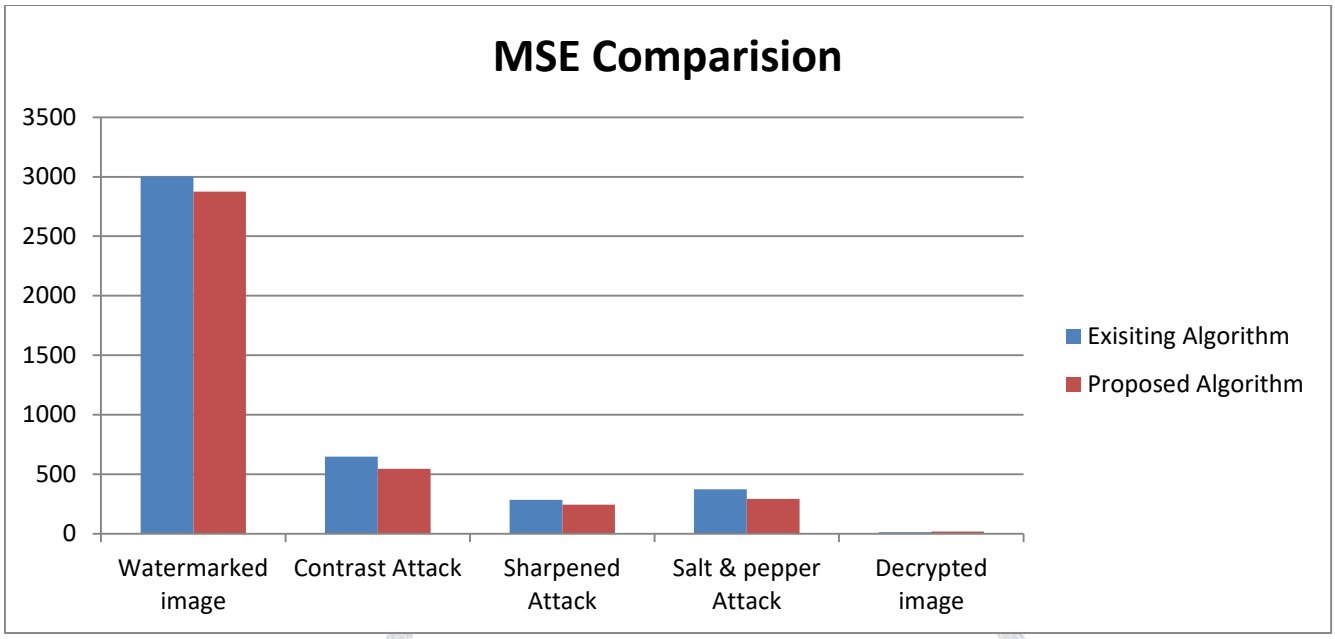

Fig 4: MSE Comparison

As shown in figure 4, the MSE value of the proposed and existing algorithm is compared under certain situations like contrast attack, sharpen attack, salt & pepper attacks. The decrypted image has least MSE value than other image.

Conclusion:

In this paper, the efficiency of the watermarking approach is concluded as it hides all the sensitive information which is stored in the form of images. In this research paper, GLCM and PCA algorithm has been utilized in order to improve the working capability of the neural network based watermarking technique. The extracted features of an image are selected by the PCA algorithm and the features of the original image are extracted by the GLCM algorithm. The scaling factor defines the output of the PCA algorithm which is used for implementation. On the basis of simulation results it is concluded that proposed algorithm performs well in terms of PSRN and MSE.

References:

[1]T. Vimala, "Salt and Pepper Noise Reduction Using Mdbtum Filter With Fuzzy Based Refinement", IJMIE, Volume 2 Issue 5, 2012

[2] D. Gabor, "Theory of communication," Journal of Institution of Electrical Engineers, vol. 93, pp. 429–457, 1946.

[3] J. Ilonen, J.-K.Kamarainen, P. Paalanen, M. Hamouz, J. Kittler, and H. K¨ alvi¨ ainen, "Image feature localization by multiple hypothesis testing of Gabor features," IEEE Trans. on Image Processing, vol. 17, no. 3, pp. 311–325, 2008.

[4] J. Ilonen, J.-K.Kamarainen, and H. K ¨ alvi¨ ainen, "Fast extraction of multi-resolution gabor features," in 14th IntConf on Image Analysis and Processing (ICIAP), 2007, pp. 481–486.

[5] E. Simoncelli, W. Freeman, E. Adelson, and D. Heeger, "Shiftablemultiscale transforms," IEEE Transactions on Information Theory, vol. 38,no. 2, pp. 587–607, 1992.

[6] J. Sampo, J.-K.Kamarainen, M. Heili ¨ o, and H. K¨ alvi¨ ainen, “Measuring translation shiftability of frames,” Computers & Mathematics with Applications, vol. 52, no. 6-7, pp. 1089–1098, 2006.

[7] Al-Haj, Ali. "Combined DWT-DCT digital image watermarking." Journal of computer science 3, no. 9 (2007): 740.

[8] Singh, Surya Pratap, PareshRawat, and SudhirAgrawal. "A robust watermarking approach using DCT-DWT." International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 8 (2012).

[9]Mansouri, A., A. MahmoudiAznaveh, and F. TorkamaniAzar. "SVD-based digital image watermarking using complex wavelet transform." Sadhana 34, no. 3 (2009): 393-406.

[10] Anthony T.S.Ho et.al, “A Robust Digital Image-in-Image Watermarking Algorithm Using the Fast Hadamard Transform”, Springer, 2011

[11] Alexander Sverdlov, “Secure DCT-SVD Domain Image Watermarking: Embedding Data in All Frequencies”, Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003

[12] T. Serre, L. Wolf, S. Bileschi, M. Riesenhuber, and T. Poggio, “Object recognition with cortex-like mechanisms,” IEEE Trans. on PAMI vol. 29, no. 3, 2007.