Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 7, July 2019, pg.146 – 151

Secure Cloud Resources Using GLCM Based Watermarking Technique

Vaishali[1]; Apneet Kaur[2]
Computer Science and Engineering, USET, RBU, MOHALI
vishalibedi92@gmail.com; Apneet@rayatbahra.com

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. Among all the proposed methods the watermarking technique is the most common technique for protecting the multimedia data for unauthorized access. A novel method is proposed which deals with secure extraction of data by utilizing transfer based image watermarking techniques. The image is embedded with a watermark using a combination of Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) in this scheme. To embed the water mark in the image simply changes the coefficient value of these transforms according to the watermark and the inverse transform is applied to the original image. These methods are too complicated and require more computational power. These methods are also provides more reverts to the security attacks. Another method is GLCM technique.

Keywords— Watermarking, DWT, PCA

I. 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 [2]. 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 [3]. 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 [4]. 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. Digital watermarks are classified according to their applications [5]. The watermarks are classified as perceptible watermarks and imperceptible watermarks, robust and fragile, public and private. Perceptible watermarks are visible to human eye while imperceptible watermarks are invisible. The perceptible watermarks are useful for primary application i.e. for statement ownership or authorship. So for this reason it should be visible. .On the other hand imperceptible watermarks are useful for complex applications such as document identification in which content being watermarked must appear in unchanged

from Examples of visible (perceptible) watermarks are logos on TV, IBM watermark and that of invisible (imperceptible) watermarks are ATT, NEC/MIT, UU etc. Perceptible watermarks i.e. visible one are extension of the concept of logos. They are applicable to images only. These watermarks are useful for content or author authentication and for detecting unauthorized copier [6]. Robust or fragile is nothing but degree to which watermarks can withstand any modifications of any types caused due to the transmission or loss compression. Perceptible watermarks are more robust in nature than imperceptible one. Robust watermarks are those watermarks which are difficult to remove from the object in which they are embedded. Fragile watermarks are those watermarks which can be easily destroyed by any attempt to tamper with them. Fragile watermarks are destroyed by data manipulation [7]. Private watermarks requires at least original data to recover watermark information Public watermarks requires neither original data nor embedded watermarks to recover watermark information. Private watermarks are also known as secure watermarks. To read or retrieve private watermark, it is necessary to have secret key. Public watermark can be read or retrieve by anyone using specialized algorithm. In this sense public watermarks are not secure. Public watermarks are useful for carrying IPR information. They are good alternatives to labels [8]. 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. 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 [9]. As of this writing, a counterfeiting scheme has been demonstrated for a class of invertible, feature-based, frequency domain, invisible watermarking algorithms. This counterfeiting scheme could be used to subvert ownership claims because the recovery of the digital signature from a watermarked image requires a comparison with an original. The counterfeiting scheme works by first creating a counterfeit watermarked copy from the genuine watermarked copy by effectively inverting the genuine watermark.

II. LITERATURE REVIEW

Nikita Kashyap, et.al (2012) introduced [10] about implemented a robust image watermarking technique for the copyright protection based on 3-level discrete wavelet transform (DWT). In this technique a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. The insertion and extraction of the watermark in the grayscale cover image is found to be simpler than other transform techniques. The proposed method is compared with the 1-level and 2-level DWT based image watermarking methods by using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE). The experimental results demonstrate that the watermarks generated with the proposed algorithm are invisible and the quality of watermarked image and the recovered image are improved.

Navnidhi Chaturvedi, et.al (2012) described about the authenticity & copyright protection are two major problems in handling digital multimedia [11]. The Image watermarking is most popular method for copyright protection by discrete Wavelet Transform (DWT) which performs 2 Level Decomposition of original (cover) image and watermark image is embedded in Lowest Level (LL) sub band of cover image. Inverse Discrete Wavelet Transform (IDWT) is used to recover original image from watermarked image. And Discrete Cosine Transform (DCT) which convert image into Blocks of M bits and then reconstruct using IDCT. In this paper we have compared watermarking using DWT & DWT-DCT methods performance analysis on basis of PSNR, Similarity factor of watermark and recovered watermark.

Surya Pratap Singh, (2012) presented [12] 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.

T. Vimala, (2012) proposed a Modified Decision Based Unsymmetrical Trimmed Median Filter (MDBUTMF) followed [13] by Fuzzy Noise Reduction Method (FNRM) for the restoration of color images that are highly corrupted by salt and pepper noise. The proposed filter (MDBUTMF) replaces the noisy pixel by trimmed median value when some of the elements with values 0"s and 255"s are present in the selected window. The throughput of FNRM is a fully noise removed image. Simulation results show the feasibility of the proposed method. The proposed method is tested. Against different color images and it gives excellent Peak Signal-to-Noise Ratio (PSNR) than the Median Filter (MF), Switching Median Filter (SMF), Boundary Discriminative Noise Reduction Algorithm (BDNRA), Decision Based Algorithm (DBA), and Decision Based Unsymmetric Trimmed Median Filter (DBUTMF).

Anthony T.S.Ho et.al (2011) proposed [14] a robust image-in-image watermarking algorithm based on the fast Hadamard transform (FHT) for the copyright protection of digital images. Most current research makes use of a normally distributed random vector as a watermark and where the watermark can only be detected by cross-correlating the received coefficients with the watermark generated by secret key and then

comparing an experimental threshold value. However, the FHT image in-image method involves a "blind" watermarking process that retrieves the watermark without the need for an original image present. 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 [15] 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 by the singular values of a visual watermark. It is shown 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.

III. RESEARCH METHODOLOGY

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.

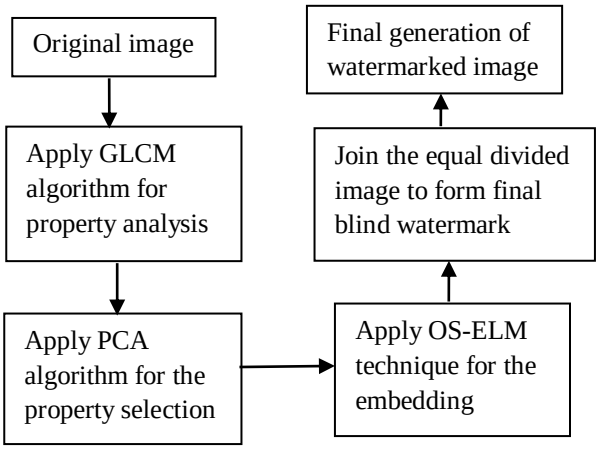

Fig 1: Proposed Flowchart of embedding

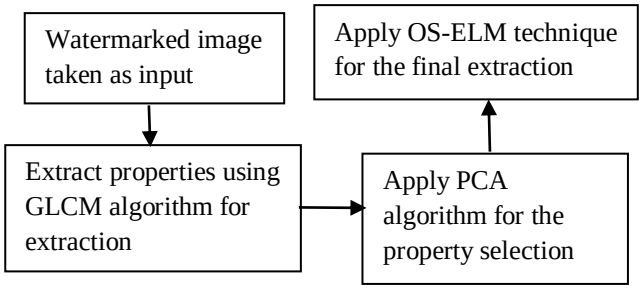

Fig 2: Proposed Flowchart for extraction

IV. EXPERIMENTAL RESULTS

The proposed research is implemented in MATLAB and the results are evaluated by comparing proposed and existing techniques with respect to certain parameters.

TABLE I
Result comparison

	Parameter values	DWT Technique	GLCM Algorithm
Watermarked image	PSNR	13.3917	18.0129
	MSE	3001.26	2874.83
	Correlation Coefficient	0.01	0.01
Contrast Attack	PSNR	20.0542	26.0537
	MSE	647.22	547.30
	Correlation Coefficient	0.96	0.01
Sharpened Attack	PSNR	23.6209	29.4842
	MSE	284.70	243.80
	Correlation Coefficient	0.97	0.98
Salt & pepper Attack	PSNR	22.4476	27.484
	MSE	373.00	293.80
	Correlation Coefficient	0.96	0.91

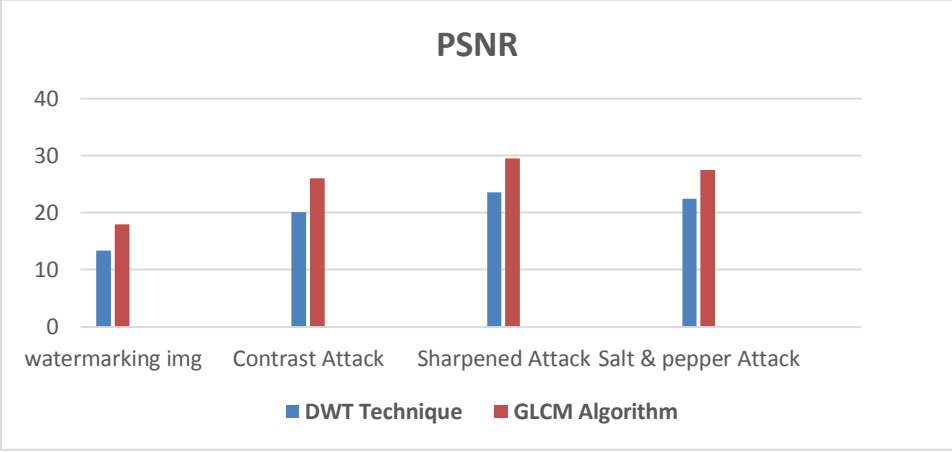

Fig 3: PSNR Comparison

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.

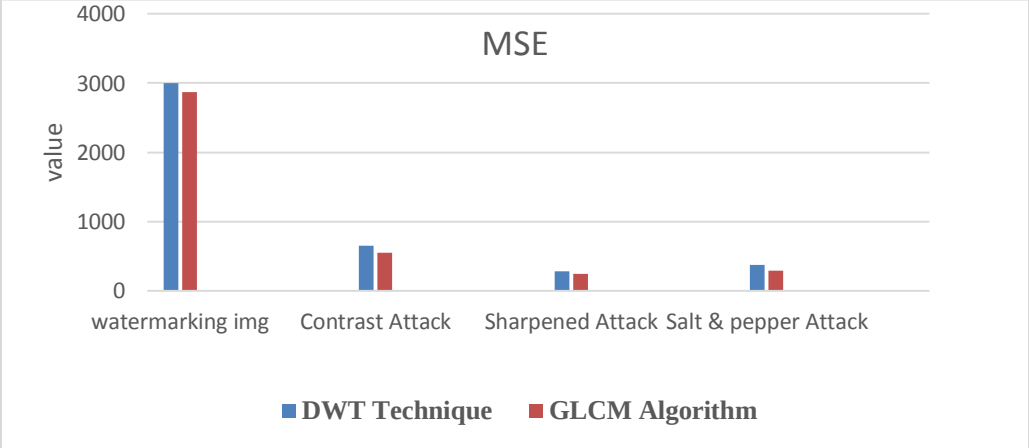

Fig 4: MSE Comparison

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.

V. 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] S.Zhang and M.A.Karim, "Anew impulse detector for switching Median filters", IEEE signal process. Lett, vol.9, no.11, pp. 360-363, Nov.2002.

[8] P. E. Ng and K. K. Ma, "A switching median filter with boundary discriminative noise detection for extremely corrupted images," IEEE Trans. Image Process., vol. 15, no. 6, pp. 1506–1516, Jun.2006.

[9] K. S. Srinivasan, D. Ebenezer, " A New Fast and Efficient Decision Based Algorithm for Removal of High-Density Impulse Noises," IEEE Signal Processing Papers, Vol. 14, No. 3, pp. 189-192, March 2007.

[10] Kashyap, Nikita, and G. R. Sinha. "Image watermarking using 3-level discrete wavelet transform (DWT)." International Journal of Modern Education and Computer Science (IJMECS) 4.3 (2012): 50.

[11] Chaturvedi, Navnidhi, and S. J. Basha. "Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the Basis of PSNR." image 2 (2012): 1.

[12] 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).

[13] J.-K. Kamarainen, V. Kyrki, and H. K ¨ alvi¨ ainen, "Invariance properties of Gabor filter based features - overview and applications," IEEE Trans. on Image Processing, vol. 15, no. 5, pp. 1088–1099, 2006.

[14] 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.

[15] 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.

