ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Improved Protection Using Self-Recognized Image

Sanchit Shrikant Mahajan, Prof. Pratima Bhati

Research scholar, Department of Computer Engineering, D.P.C.O.E, Savitribai Phule Pune University, India

Professor, Department of Computer Engineering, D.P.C.O.E, Savitribai Phule Pune University, India

ABSTRACT: The protection of data can be done by several mechanism to secure and achieve authenticity and integrity of data. Data hiding is a technique in which a piece of information can be embedded to cover media data for security reason. So a digital watermarking can be used to protect the copyright of digital products. In such processes it is needed to maintain the original view of the host image. For evaluating the watermarking methods performance it must be concentrate on the robustness of watermarked image quality and restored image quality. For this purpose the preinserted encoding mechanism can be used in the discrete cosine transform domain. So a simulator preinserted code can address the next level of protection to perform various procedures for the sake of integrity and security.

KEYWORDS: Digital watermark, Pre-inserted code, Data hiding, Blind watermark.

I. INTRODUCTION

The techniques used to embed information to protect the legal copyright of various forms of multimedia are needed today. The data hiding techniques focus on how to efficiently embed a piece of information into cover media data to carry out security. The digital watermarks have gain importance in protecting the copyright of digital products. The efficient watermarking techniques require visual imperceptibility and robustness against various attacks. For this purpose a novel self recognized and crop resistant watermarking methods provide the visual quality of the embedded image. For embedding a pre-inserted encoding method to mark the original position of the watermark, the method is able to locate the embedded watermark and retrieve it even in the event of a synchronous cropping attack. This blind watermark extraction uses a voting mechanism to retrieve exact watermark information and recover the original unmarked image without knowledge of the host image. To restore an original image, the method can obtain the host image information, recover the host image under resist multiform attacks, and thus protect the copyright of digital products. Based on the pre-inserted encoding system, this method can identifies the watermark sequence correctly. The embedding watermarks involves two key tasks, first authenticating copyright protection and maintaining the original view of the carrier image. To protect the copyright of an image, a watermarking mechanism must be robust enough to resist malicious attacks even if the watermarked image has been attacked. Also the watermarked images quality must be good so that it is difficult for an intruder to distinguish between the host image and the embedded one. In addition, the embedded information should not seriously distort the protected image, which may degrade the images quality. At the time of evaluating a watermarking mechanisms performance, we have to concentrate on issues like, robustness, the watermarked images quality, and the restored images quality.

II. LITERATURE SURVEY

To guarantee the visual quality of embedded images, it is important to make sure that the host image remains visually similar to the original image after embedding. The previous work done by C.C.Chang et al., and X.You et al., for maintaining the quality of watermarked image and restored image. There were two schemes used for restoring unmarked images, reversible and removable methods, by these scientists. But the reversible methods and removable methods still unable to achieve the robustness and quality of the restored image. So it is necessary to implement better scheme to enhance the robustness and also guarantee the least impact on the embedded image.

.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

A.M. Alattar in [1] used a very high-capacity algorithm based on the difference expansion of vectors of arbitrary size developed for embedding a reversible watermark with low image distortions. A reversible watermarking algorithm with very high data-hiding capacity has been developed for color images. The algorithm restores the exact original image, hides several bits. The reversible integer transform and the other conditions to avoid underflow and overflow are derived for any vector of arbitrary length. To maximize the amount of data that can be hidden into an image, the embedding algorithm applied across the color components. The experimental results indicate that the spatial, quad-based algorithm allows for hiding the largest payload at the highest signal-to-noise ratio. Also indicates that the amount of data one can embed into an image depends highly on the nature of the image. The test results also indicate that the performance of the spatial, quad-based algorithm is superior to that of the spatial, triplet based algorithm at higher PSNR. These results also show that applying the algorithm across the color components has inferior performance to applying the algorithm spatially; hence, cascading cross-color with spatial applications would be useful only when there is a need to hide a large amount of data without regard to the quality of the watermarked image.

In [2] C.C. Chang et.al., presented a lossless and reversible steganography scheme for hiding secret data in each block of quantized discrete cosine transformation (DCT) coefficients in JPEG images. This shows that the two successive zero coefficients of the medium-frequency components in each block are used to hide the secret data. Also it modifies the quantization table to maintain the quality of the image. The results also confirm that the proposed scheme can provide expected acceptable image quality of images and successfully achieve reversibility. DCT is a widely used mechanism for frequency transformation. To extend the variety of cover images and for the sake of repeated usage, they over a lossless data hiding scheme for DCT-based compressed images. Using a modified quantization table and our proposed embedding strategy, the proposed scheme can maintain the image quality of images, with a PSNR value 2.2 times higher than that ordered by a standard quantization table without affecting hiding capacity. The experimental results further demonstrate that the proposed scheme provides images with acceptable image quality and hiding capacity.

C.C. Chang et.al., in [3] presented a reversible data hiding scheme based on side match vector quantization (SMVQ) for digitally compressed images. With this method receiver performs two steps to achieve - extract the secret data and reconstruct the original SMVQ compression codes. The results show that the performance of this proposed scheme is better than those of other information hiding schemes for VQ-based and SMVQ-based compressed images. The experimental results also provides effectiveness and reversibility of the proposed scheme. Hiding data in SMVQ-compressed codes originally caused a large distortion in stego-images because SMVQ is a low bit-rate compression scheme. To maintain the advantages of SMVQ and make sure the original compression indexes can be successfully reconstructed after secret data are extracted, they hide the secret data in compressed image and achieve reversibility. The original compressed image can be completely reconstructed after hidden secret data extraction, and the original compressed codes can be stored directly and used repeatedly. In addition, the proposed scheme can simply hide or extract the secret data and restore the SMVQ-compressed codes without complex computations. The hidden secret data can also be extracted from the stego-image without referencing the original compressed cover image. So proposed method is superior to that of other VQ or SMVQ-based reversible hiding schemes.

M.U. Celik et.al., in [4] presented a novel framework for lossless authentication watermarking enables zero-distortion reconstruction of un-watermarked images upon verification. They presented a new lossless image authentication framework which offers computational efficiency, public/private key support and improved tamper-localization accuracy. The proposed method is flexible and compatible with the existing lossless data embedding and fragile image authentication algorithms. This new framework allows validation of the watermarked images before recovery of the original image. This decreases computational work when verification step fails or the zero-distortion reconstruction is not needed. For authenticated images the integrity of reconstructed image is ensured by uniqueness of the reconstruction procedure. The framework also enables public(-key) authentication without granting access to the perfect original and allows for efficient tamper localization. Also the effectiveness of this method is demonstrated by implementing the scheme using hierarchical image authentication along with lossless generalized-least significant bit data embedding.

In [5] C.C. Chang et.al., proposed a novel watermarking mechanism by utilizing Pair difference correlations upon subsampling and the technique of JND. The simulation results revealed that the new scheme approximated a lossless watermarking scheme. Also the novel scheme resisted various signal processing attacks and geometric transformation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

attacks; therefore, it can be used to protect the ownership of important watermarked images. Furthermore, the novel method permitted authorized users to extract and restore the watermarked image without the host image. The new scheme confirms the essentials of robustness and restored image fidelity, which are practical for preserving valuable images.

C.Y. Lin et.al., in [6] presented an effective technique for image authentication which can prevent malicious manipulations but allow JPEG lossy compression. The authentication is based on invariance of relationships between discrete cosine transform coefficients at the same position in separate blocks of an image. These relationships are preserved when discrete cosine transform coefficients are quantized in JPEG compression. This proposed method can distinguish malicious manipulations from JPEG lossy compression regardless of the compression ratio or the number of compression iterations. They described adaptive methods with probabilistic guarantee to handle distortions introduced by various acceptable manipulations. They also present theoretical and experimental results to demonstrate the activeness of the technique.

P. Bas et.al., in [7] presented a new approach for watermarking of digital images providing robustness to geometrical distortions. A new class of watermarking schemes using the image content is presented. They propose an embedding and detection scheme where the mark is bound with a content descriptor defined by salient points. The embedding process of the signature is done by extracting feature points of the image and performing a Delaunay tessellation on the set of points. The mark is embedded using a classical additive scheme inside each triangle of the tessellation. The detection is performed using correlation properties on the different triangles. The performance of the presented scheme is evaluated after JPEG compression, geometrical attack and transformations. The final results show that the fact that the method is robust to different manipulations. The presented method is robust to the Stir Mark attack, shearing distortion, JPEG compression, and slight global transformations. But drawback of this technique is that the robustness depends on the capacity of feature point detector.

In [8] C.S. Lu et.al., proposed a scheme that can resist two famous water- mark estimation-based attacks, which have successfully cracked many existing watermarking schemes. The false negative and false positive analyses are conducted to verify the performance of scheme. A novel watermarking approach, called the non blind embedder, has applied by exploiting the available information of denoising-based watermark prediction. The information obtained using shrinkage-based denoising (soft-thresholding) techniques is easy to control, and, that denoising itself is, in fact, a solution for oblivious watermark detection. The knowledge at the detector side can then be utilized to design a nonblind embedder, which is extremely advantageous over the common blind embedders. The performance of scheme, composed of a non-blind embedder and a blind detector, has also been analyzed regarding false negative and false positive probabilities.

In [9] J. Barr et.al., developed a system which will mitigate the threat posed by the copy attack. They first developed an image signature algorithm which uses highly stable low frequency DCT coefficients to uniquely describe the image. This image signature was then combined with a standard image watermark, and embedded into the original image. If an attacker attempts to remove the watermark from this image and insert it into a new image, the image signature embedded in the watermark will not match the re-calculated image signature of the new image. The watermark also enables geometric synchronization, which allows us to automatically restore the image to its proper rotation, scale, and translation. This process, which in other systems must be performed by hand, is necessary to ensure the re-calculated image signature matches the image signature of the original digital image.

Q. Cheng et.al., in [10] presented an investigation on robust optimum detection of multiplicative watermarks. In this the novel optimum detectors for multiplicative watermarks are derived using locally optimum detection for the generalized Gaussian distributions. For sub-band transformed domains such as the discrete cosine transform, discrete wavelet transform, and pyramid transform, a class of generalized correlators is constructed based on the generalized Gaussian distributions. For this, the square-root detector is designed and demonstrated to have near optimal performance for a large set of images and employed as a universally optimal detector or decoder for images and video. The locally most powerful detection method is then extended to DFT domain multiplicative watermarking with magnitudes of coefficients modeled by the Weibull distributions. The another class of detectors is built based on this statistical

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

modeling. The robust optimum detection of multiplicative watermarks can be applied to copyright notification, enforcement, and broadcast monitoring. They applied the robust optimum watermarking detection to combined audio and video watermarking. It can tolerate commonly used audio and video compressions but is sensitive to content changes. It can be applied to audiovisual content authentication in commerce, law, defense, and journalism.

In [11] C.S. Lu et.al., proposed a new digital signature scheme which makes use of an images contents to construct a structural digital signature for image authentication. For image authentication, it is desired that the verification method be able to resist content-preserving modifications while being sensitive to content-changing modifications. The characteristic of the SDS is that it can tolerate content-preserving modifications while detecting content-changing modifications. There are many incidental manipulations that bypassed in the proposed scheme. Performance analysis is conducted and experimental results show that the new scheme is indeed superb for image authentication.

S. Craver et al., in [12] addresses the capability of invisible watermarking schemes to resolve copyright ownership. They show that, in certain applications, rightful ownership cannot be resolved by current watermarking schemes alone. Specifically, it attack existing techniques by providing counterfeit watermarking schemes that can be performed on a watermarked image to allow multiple claims of right ownership. In order to protect against the counterfeiting techniques that they develop, it examine the properties necessary for resolving ownership via invisible watermarking. Also introduced and studied invertibility and quasi-invertibility of invisible watermarking techniques. They proposed noninvertible watermarking schemes, and subsequently give examples of techniques that are invulnerable against more sophisticated attacks.

In [13] X. You et al. proposed a new method for constructing nontensor product wavelet filter banks and applied them into watermarking scheme design. The new nontensor product wavelet filter banks are constructed according to special symmetric matrix. They overcome the drawback of tensor wavelet banks which can reveal the singularities in the three directions only. Based upon the nontensor filter banks they construct, empirical studies have been conducted to show the capability of nontensor product wavelet filter banks in revealing the singularities in various directions of image. Accordingly, they developed a modified significant difference watermarking scheme, whose performance shows the superiority of the nontensor product wavelet-based watermarking in terms of robustness and m-perceptibility. The proposed wavelet filter banks make the watermarking scheme more flexible because more sub-bands and coefficients are suitable for watermark embedding. The experimental results shown that the proposed algorithm is robust against various attacks.

III. CONCLUSION

We have to develop a strong enough system which will overcome the limitations of existing watermarking methods and maintains the highest visual quality of the embedded image and also robust against various malicious attacks..

IV. ACKNOWLEDGEMENTS

Sincere thank to the reviewers for reviewing this manuscript and providing inputs for greatly improving the quality of this paper.

REFERENCES

[1] A.M. Alattar, “Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform”, IEEE Trans. Image Processing, vol. 13, no. 8, pp. 11471156, 2004.
[2] C.C. Chang et al., Reversible Hiding in the DCT Based Compressed Images, Information Sciences, vol. 177, no. 13, pp. 27682786, 2007.
[3] C.C. Chang,W.L. Tai, and C.C. Lin, A Reversible Data Hiding SchemeBased on Side Match Vector Quantization, IEEE Trans. Circuits and System for Video Technology, vol. 16, no 10,,pp. 13011308, 2006.
[4] M.U. Celik, G. Sharma, and A.M. Tekalp, Lossless Watermarking for Image Authentication: A New Framework and an Implementation, IEEE Trans. Image Processing, vol. 15, no. 4, pp.10421049, 2006.
[5] C.C. Chang, P.Y. Lin, and J.S. Yeh, Preserving Robustness and Removability for Digital Watermarks Using Sub sampling and Difference Correlation, Information Sciences, vol. 179, no. 13, pp. 22832293, 2009.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

[6] C.Y. Lin and S.F. Chang, A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation, IEEE Trans.Circuits and and systems for Video Technology, vol. 11, no.2, pp.153168, 2001.
[7] P.Bas, J.M. Chassery, and B. Macq, Geometrically Invariant Watermarking Using Feature Points, IEEE Trans. Image Processing, vol. 11, no. 9, pp. 10141028, 2002.
[8] C.S.Lu, H.Y. Liao, and M. Kutter, Denoising and Copy Attacks Resilient Watermarking by Exploiting Prior Knowledge at Detector, IEEE Trans. Image Processing, vol. 11, no. 3, pp. 280292, 2002.
[9] J. Barr, B. Bradley, and B.T. Hannigan, Using DigitalWatermarks with Image Signatures to Mitigate the Threat of the Copy Attack, Proc. Intl Conf. Acoustics,
[10] Q. Cheng and T.S. Huang, Robust Optimum Detection of Transform Domain Multiplicative Watermarks, IEEE Trans. Signal Processing, vol. 51, no. 4, pp. 906924, 2003.
[11]C.S.Lu and H.-Y.M. Liao, Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme, IEEE Trans. Multimedia, vol. 5, no. 2, pp. 161173, 2003.
[12] S. Craver et al., Resolving Rightful Ownership with Invisible Watermarking Techniques: Limitations, Attacks and Implications, IEEE J.Selected Areas in Comm., IEEE Press, pp. 573586, 1998.
[13] X. You et al., A Blind Watermarking Scheme Using New Nontensor Product Wavelet Filter Banks, EEE Trans. Image Processing, vol. 19, no. 12, pp. 32713284, 2010.
[14] Jung-San Lee and Bo Li, Self-Recognized Image Protection Technique that Resists Large- Scale Cropping, 2014 IEEE Computer Society.

BIOGRAPHY

Sanchit Shrikant Mahajan is a M.E. student in the Computer Engineering Department, Dhole Patil College of Engineering, Savitribai Phule University Pune. He received Bachelor degree in Computer Science and Engineering stream (B.E.-C.S.E.) in 2009 from Shivaji University, Kolhapur, Maharashtra, India. His research interest is Image Processing.