ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

SECURE WATERMARKING FOR IMAGE TRANSACTION AND IDENTIFY OWNERSHIP

P.Jagadheesan,

PG scholar-ME(EST),

Excel college of Engineering & Technology

D.Viji M.E,

Assistant Professor,

Excel college of Engineering & technology

ABSTRACT

Privacy is a critical issue when the data owners outsource data storage or processing to a third party computing service, such as the cloud. In this paper, we identify a cloud computing application scenario that requires simultaneously performing secure watermark detection and privacy preserving multimedia data storage. We then propose a compressive sensing (CS)-based framework using secure multiparty computation (MPC) protocols to address such a requirement. In our framework, the multimedia data and secret watermark pattern are presented to the cloud for secure watermark detection in a CS domain to protect the privacy. During CS transformation, the privacy of the CS matrix and the watermark pattern is protected by the MPC protocols under the semi-honest security model. We derive the expected watermark detection performance in the CS domain, given the target image, watermark pattern, and the size of the CS matrix (but without the CS matrix itself). The correctness of the derived performance has been validated by our experiments. Our theoretical analysis and experimental results show that secure watermark detection in the CS domain is feasible. Our framework can also be extended to other collaborative secure signal processing and data-mining applications in the cloud.

I.INTRODUCTION

A digital watermark is an invisible signature embedded inside an image to show authenticity and ownership. An effective digital watermark should be perceptually invisible to prevent obstruction of the original image. It should be statistically invisible to prevent detection, and it should also be robust to many image manipulations, such as filtering, additive noise, and compression. Digital Watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has been proposed as a new, alternative method to enforce the intellectual property rights and protect digital media from tampering. It involves a process of embedding into a host signal a perceptually transparent digital signature, carrying a message about the Signature is called the digital watermark.

Digital watermarking techniques may be classified in several ways

Robustness

A digital watermark is called "fragile" if it fails to be detectable after the slightest modification.

Perceptibility

A digital watermark is called imperceptible if the original cover signal and the marked signal are perceptually indistinguishable.

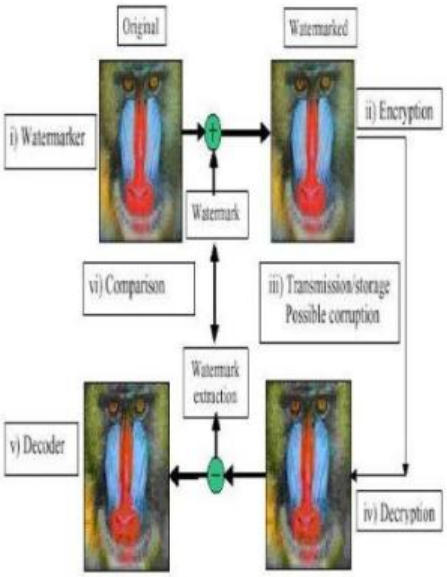
II.WATERMARKING EXTRACTION

The increasing amount of applications using digital multimedia

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

technologies has accentuated the need to provide copyright protection to multimedia data. Digital watermarking is a method that has received a lot of attention in the past few years. A digital watermark can be described as a visible or preferably invisible identification code that is permanently embedded in the data . It means that it remains present within the data after any decryption process. A general definition can be given !"Hiding of a secret message or information within an ordinary message and theextraction of it at its destination. !"Complementary to encryption, it allows some protection of the data after decryption. As we know, encryption procedure aims at protecting the image (or other kind of data) during its transmission.

Figure1.watermarking extraction

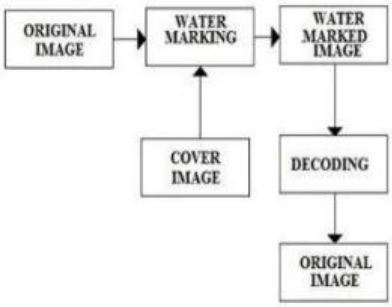


The purpose here is to forbid any unauthorized use of an image by adding an obvious identification key, which removes the image's commercial value. On the other hand, invisible watermarks are used for content and/or author identification in order to be able to determine the origin of an image. They can also be used in unauthorized image's copies detection either to prove ownership or to identify a customer.

III.Existing system

Digital watermarking is a technique used for protecting intellectual property rights of digital media owners. Watermarking embeds a signal into the data stream that is imperceptible to the human observer, but can be detected by a watermark detector, hence identifying the owner and possibly the customer to whom this copy was origi-nally distributed.The water mark does not prevent a user from listening.

Frigure2:block diagram of existing system



The collusion problem was first addressed by Swanson et al., who presented a scene-based image watermarking technique that is robust to self-collusion attacks. In their technique, the image sequence is segmented to different scenes and a temporal wavelet transform is applied to the frames in each scene. The watermark is added to the low-pass and high-pass frames of the temporal wavelet transform. They compute the 8 × 8 DCT of those frames and use the perceptual masking properties of the human visual model to embed an invisible and robust watermark. Their method uses a two-level hierarchy of transforms and is considered to be highly complex. Recent work by Trappe et has focused on collusion-resistant digital fingerprinting that can identify colluders; their work makes use of effective anti-collusion codes for CDMA-type

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

watermarking using the theory of combinatorial designs.

IV. Proposed system

The performance of any watermarking scheme relies heavily on the design of the watermark detector. Zeng et al. argued that for the particular application of resolving rightful ownership using invisible watermarks, it is crucial that the original image not be directly involved in the watermark detection process. The true owner should be able to detect the watermark without using a second image, since its authenticity is also questionable. Hernandez et al. presented a watermark detection algorithm whereffi the embedding domain is the DCT coe cients except the dc term. Their algorithm assumes a generalizedffi Gaussian distribution for the ac coe cients of the DCT and an additive embedding rule.Nikolaidis et al. considered watermark-ing in the DCT and DWT domainsffiand the same pdf assumption for the coe cients.

The selection of the coeffi cient in the i^{th} macroblock for watermark embedding is under the control of a key. If the same key is used for every frame, the watermarking algorithm becomes vulnerable to a self-collusion attack. Thus, a very long key stream sequence is required. Transmitting a long key, however, would make the algorithm impractical. This problem is solved by generating the key from a combination of a public key, Kp_i, extracted from some features of the macroblock, and a secret key, Ks, possessed by the copyright owner. The public key is extracted from each macroblock and passed as the plaintext to a cryptographic system with the secret key, Ks. The ciphertext generated by the cryptographic system is the key for that macroblock.

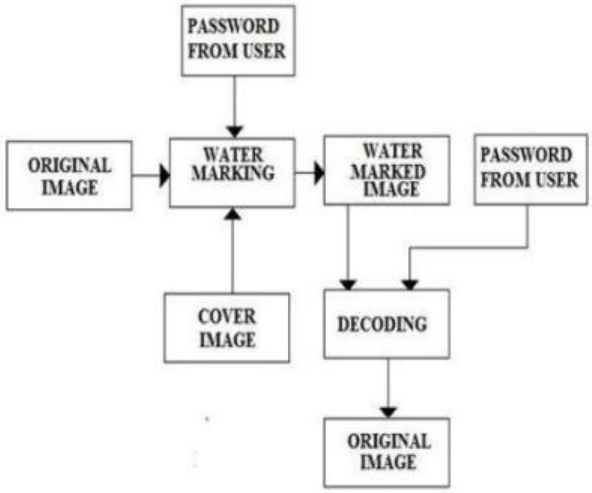


Figure3:block diagram of proposed system

Since the security demands of watermarking systems are less than those of cryptographic systems, a fast and simple cryptographic scheme can be used for this purpose. We used a shift cipher with modulus 2, key Ks, and plaintext Kp_i. Two bits of this key determine the selected 8 ×8 block in the macroblock, $b8_i$, another two bits determine the selected 4 × 4 block in the 8 × 8 block, $b4_i$, and four bits determine the selected ac quantized residual in that 4 × 4 block, cw_i, for watermark embedding.Kp should be extracted from some features of the macroblock that cannot be changed by the attacker without degrading the perceptual quality of the image. In the next section, we describe the public key extraction procedure. Figure 1.6.1 shows the structure of our proposed watermarking algorithm.

Advantage

- ∑ Identify the user if attacker cannot break the message
- ∑ Secured transmission
- ∑ By user can select with encryption data

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

User set the password in selected bit in image

V.Embedding method

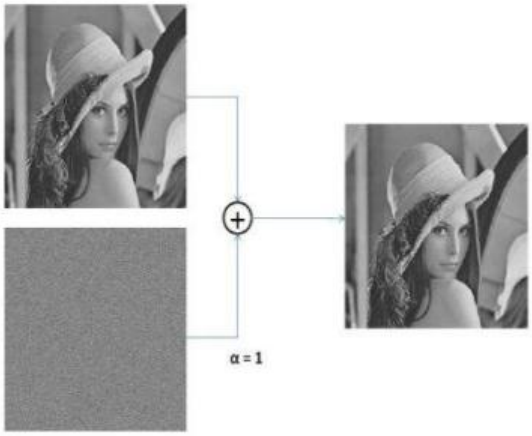
A digital watermarking method is referred to as spread-spectrum if the marked signal is obtained by an additive modification. Spread-spectrum watermarks are known to be modestly robust, but also to have a low information capacity due to host interference.A digital watermarking method is said to be of quantization type if the marked signal is obtained by quantization. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference.

Detector:

1.Calculate the linear correlation between the watermarked image that was received and the initial reference pattern

2.Decide what the watermark message was, according to the result of the correlation. If the linear correlation value was above a threshold, we say that the message was a 1. If the linear correlation was below the negative of the threshold we say that the message was a 0. If the linear correlation was between the negative and the positive threshold we say that no message was embedded.

Figure4:Embeeding process



Methodology

Figure5.imageProcessing

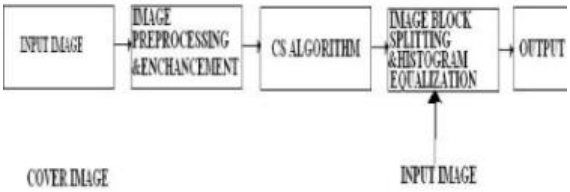


Image preprocessing & enhancement:

Image pre-processing is the term for operations on images at the lowest level of abstraction. These operations do not increase image information content but they decrease it if entropy is an information measure.The aim of pre-processing is an improvement of the image data that suppresses undesired distortions or enhances some image features relevant for further processing and analysis task. Image pre-processing use the redundancy in images. Neighboring pixels corresponding to one real object have the same or similar brightness value. If a distorted pixel can be picked out from the image, it can be restorted as an average value of neighboring pixels. Image pre-processing methods can be classiØed into categories according to the size of the pixel neighborhood that is used for the calculation of a new pixel brightness.

IMAGE CROPPING AND FILTERING

The first step in image pre-processing is image cropping. Some irrelevant parts of the image can be removed and the image region of interest is focused. This tool provides a user with the size information of the cropped image. MatLab function for image cropping realizes this operation interactively waiting for an user to specify the crop rectangle with the mouse and operates on the current axes.

The output image is of the same class as the input image. The two-dimensional convolution operation is

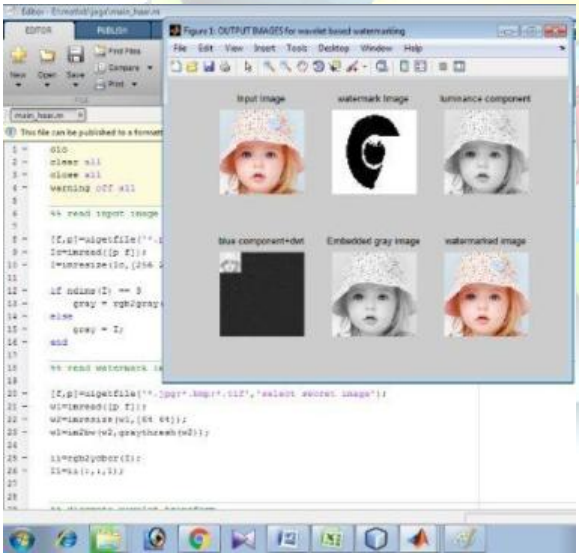
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

fundamental to the analysis of im- ages. A new value is ascribed to a given pixel based on the evaluation of a weighted average of pixel values in a k*k neighborhood of the central pixel. Convolution kernel or the Ølter mask is represented with weights supplied in a square matrix. It is applied to each pixel in an image.

CLEARRING AREAS OF A BINARY IMAGE

If there is a deformation of the expected shape and size of the border and the whole region during the separation of image object from its background, it can be partially overcome. Usually small polygon mask, located next to the region and out of it, is added to clear image area with similar brightness of the region. This mask can reshape image objects and provides a separation image objects from each other and from their image background.

Figure6:simulation results



VI.CS ALGORITHM

Compressed sensing (also known as **compressive sensing**, **compressive sampling**, or **sparse sampling**) is a signal processing technique for efficiently acquiring and reconstructing a signal, by finding solutions To prevent over-smoothing of edges and texture details and to obtain a reconstructed CS image which is accurate and robust to noise and artifacts, this method is used. First, an initial estimate of the noisy point-wise orientation field of the image I , $\hat{d}$, is obtained. This noisy orientation field is defined so that it can be refined at a later stage to reduce the noise influences

$$J_\rho(\nabla I_\sigma) = G_\rho * (\nabla I_\sigma \otimes \nabla I_\sigma) = \begin{pmatrix} J_{11} & J_{12} \\ J_{12} & J_{22} \end{pmatrix}$$

. Here, J_ρ refers to the structure tensor related with the image pixel point (i,j) having standard deviation ρ G refers to the Gaussian kernel $(0, \rho^2)$ with standard deviation ρ. σ refers to the manually defined parameter for the image I below which the edge detection is insensitive to noise. ∇I_σ refers to the gradient of the image and $(\nabla I_\sigma \otimes \nabla I_\sigma)$ refers to the tensor product obtained by using this gradient.

VII.CONCLUSION

The goal of this dissertation was to present a robust watermarking algorithm for H.264 and to address challenges in compressed-domain image watermarking.Watermarking digital image introduces challenges that are not present when water-marking digital images. The large amount of data and inherent redundancy between frames makes image watermarking algorithms susceptible to self-collusion attacks. The self-collusion attack is one of the most powerful attacks for image. we designed a novel low complexity watermarking algorithm that was robust to self-collusion attacks . The algorithm embedded the watermark in the quantized ac residuals of the H.264-compressed image. It achieved collusion resistance by em-bedding the watermark in theffsame location in similar frames and di erentffi locations in dissimilar frames. The coe cient within a macroblock that holds the watermark was determined by a key that was specific to that

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
nternational Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

macroblock, but this could require a long key stream sequence. To avoid this problem, the key was generated using a public key extracted from features of the macroblock and the copyright owner's secretff key. It was proposedffithat the relative di erence of the DC coe cients of the 4 × 4 blocks in a macroblock is a robust feature for public key extraction.

The algorithm we proposed in Chapter 2 embedded the watermark in the com-pressed image, but this algorithm was not robust against several common watermark-ing attacks besides the self-collusion. The watermark was embedded in and extracted from the I-frame quantized ac residuals, so any simple processing, such as filtering followed by reencoding by an H.264 encoder, changes the intra-macroblock predic-tion modes, and thus the residuals, which makes watermark recovery impossible. In Chapter 3, we presented a perceptual watermarking algorithm for H.264 that was robust to common signal processing attacks To achieve this goal we em-bedded the watermark in the residuals to avoid decompressing the image and also to reduce the complexity of the watermarking algorithm. However, the watermark was extracted from the decoded image sequence to make the algorithm robust to intra-prediction mode changes. Since H.264's high compression performance leaves little room for an imperceptible signal to be inserted, we employed a human visual model to increase the payload and add robustness while limiting visual distortion. Watson et al. derived a model for distortion perception in 8 × 8 DCT blocks, and we extended this human visual model for the 4 × 4ffiDCT block used in H.264. If all the coe cients with visual capacity for watermark embedding were used, the visual quality of the image would be degraded. We proposed embedding the ffiwatermark in a selected subset of the coe cients that have visual watermarking capacity by using a key-dependent algorithm. This makes the algorithm more robust to malicious at-tacks.

VIII.REFERENCE PAPER

[1] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," IEEE Signal Process. Mag., vol. 30, no. 2, pp. 87–96, Mar. 2013.

[2] Z. Erkin, A. Piva, S. Katzenbeisser, R. Lagendijk, J. Shokrollhi, G. Neven, et al., "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," EURASIP J. Inf. Security, vol. 7, no. 2, pp. 1–20, 2007.

[3] J. Eggers, J. Su, and B. Girod, "Public key watermarking by eigenvectors of linear transforms," in Proc. Euro. Signal Process. Conf., 2000.

[4] S. Craver and S. Katzenbeisser, "Security analysis of public-key watermarking schemes," in Proc. Math. Data/Image Coding, Compress., Encryption IV, Appl., vol. 4475. 2001, pp. 172–182.

[5] A. Adelsbach and A. Sadeghi, "Zero-knowledge watermark detection and proof of ownership," in Proc. 4th Int. Workshop Inf. Hiding, vol. 2137. 2001, pp. 273–288.

[6] J. R. Troncoso-Pastoriza and F. Perez-Gonzales, "Zero-knowledge watermark detector robust to sensitivity attacks," in Proc. ACM Multimedia Security Workshop, 2006, pp. 97–107.

[7] M. Malkin and T. Kalker, "A cryptographic method for secure watermark detection," in Proc. 8th Int. Workshop Inf. Hiding, 2006, pp. 26–41.

[8] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," IEEE Trans. Image Process., vol. 8, no. 11, pp. 1534–1548, Nov. 1999.