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. 4, Issue 1, January 2016

Image Authentication System Using Fused Watermarking Technique

K.Balasamy, M.Divya Dharshini, S.Gayathri, M.Mowna Geetha

Assistant Professor, Dept. of. I.T, Dr. Mahalingam College of Engineering and Technology, Coimbatore, India

Student, Dept. of. I.T, Dr. Mahalingam College of Engineering and Technology, Coimbatore, Pollachi, India

Student, Dept. of. I.T, Dr. Mahalingam College of Engineering and Technology, Coimbatore, Pollachi, India

Student, Dept. of. I.T, Dr. Mahalingam College of Engineering and Technology, Coimbatore, Pollachi, India

ABSTRACT:In order to improve the robustness of watermarking algorithm, a dual watermarking method is proposed to provide protection. For protecting various online resources from unauthorized users, visible watermarking is more importanthowever robust, for illegal removal and other common signal processing and geometric attacks, visiblewatermarks are vulnerable. Visible watermark images can be enhanced by multiple invisible watermarks. If image is tampered, the invisible watermark can be extracted. In case of multiple watermark, one watermark can be survived under different attacks. Usually, extraction is the first step for image authentication. Before extraction two images are fused using arithmetic blend extension method. The watermark extraction is done by reversing the process of arithmetic blend extension algorithm. As the result, we can get the original image and the watermarked image.

KEYWORDS: Dual Watermarking Method, Arithmetic blend extension algorithm, Fused Watermarking method

I. INTRODUCTION

Information to be embedded in a single is called a digital watermarking. Digital watermarking may be used for a wide range of application like copyright protection, tracking source, monitoringbroadcast, authentication of video. Recently, watermarking technique have been considered as one of the promising techniques for multimedia authentication. Among these, fused watermarking technique have been proposed to protect copyright and provide tamper of the content. These technique allow acceptable content preserving manipulation (i.e., changing the quality of the image without modifying the content of image) such as common processing of image(e.gImage blurring ,Gaussian low-pass filtering ,median filtering) ,while detecting content- altering manipulations such as removal, addition and changing of object. "Watermarking" is the process of hiding digital information .Fused watermark may be used to verify the authentication of the carrier signal or to show the identity Traditional watermarks can be applied to visible media (like pictures or videos), whereas in fused watermarking, the signal may be audial, visual, script or 3D. A signal may carry several different watermarks atthe same time. The watermarked content should be consumable at the intended user device without giving annoyance to the user. Watermark-detector device helps to display only the watermarked image. Only the authorized parties shall only be accessible the watermark information. Only authorized parties shall be able to alter the watermark content. Unauthorized access of the watermarked data can be prevented by encryption. The computation need for the selected algorithm should be minimum. Watermarking must be strong enough to withstand all kinds for signal processing operations. Any attempt, whether international or not, that has a potential to alter the data content is considered as an attack. Watermarking should be done in such a way that it doesn't increase the bandwidth. If watermarking becomes a burden for the available bandwidth, the method will be rejected.

II. RELATED WORK

Several methods are offered to defend the picture and to get back it where watermarked image has been tampered. To authenticate the image and recover it, these techniques insert two semi-fragilewatermarks, if tampered. All these technique have the ability of authentication and recovery of the image but at the cost of imperceptibility. However, the

DOI: 10.15680/IJIRCCE.2016. 0401036

issue with these technique is the use of watermarks, which affects the imperceptibility of the watermark. Similarly, they use semi-fragile watermark authenticating and recovering the images authentication .This approach is unable to authenticate the content and this method is up to some extend only, it will not work for jpeg image. For many applications, like semi-fragile image authentication, stego-images with high visual quality, data embedding capacity, and the toughness in data hiding scheme are acceptable. It has been successfully applied to authenticate lossless compressed JPEG2000 images, followed by possible transcoding.Not only dual protection of the image content is achieved, but also maintain higher visual quality for a specified level of watermark robustness. In real-time applications, the complete computing load is low enough to be practical. The security of medical images and reviewed some work done regarding them. Detection of tamper and subsequently recovering the image was proposed as a fragile watermarking scheme. It required a secret key and a public chaotic mixing algorithm to embed and recover a tampered image.

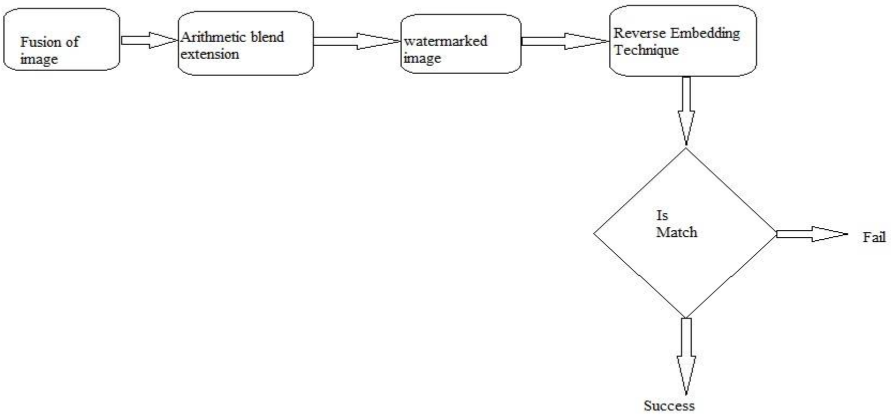


Fig 1: Block diagram for watermarking process

III. PROPOSED SYSTEM

It is a single extension method targeting the bitmap class. The Arithmetic Blend extension method expects as parameters two source/input bitmap objects and an enumeration value indicating the type of Image Arithmetic to perform. The method iterates both byte array data buffer simultaneously, having set the for loop condition to regard the array size of both byte arrays. Scenarios where byte array data buffers will differ in size occurs when the source images specified are not equal in terms of size dimensions. How each iteration increments the loop counter by a factor of four allowing us to treat each iteration as a complete pixel value. Each data buffer element represents an individual color component. Every four element represents a single pixel consisting of the components: Alpha, Red, Green and Blue.

A. *Watermark Generation*

In order to offer a protected image verificationsystem, two or more pictures are fused together to form a new image. This fusion is done by arithmetic blend extension method. In this method, addition is performed on two images corresponding pixel color components. The values resulting from performing calculations represent a lone image which is mixture of the two uniquesource.

B.*Watermark Embedding*

Fused image is then embedded with the original image. The method accesses pixel data of each image and creates copies kept in byte arrays. Each element within the byte array data buffer represents a single color components, either red, green or blue. The fused image already formed using these methods. This method is again used, which results in improve the robustness of watermarked image.

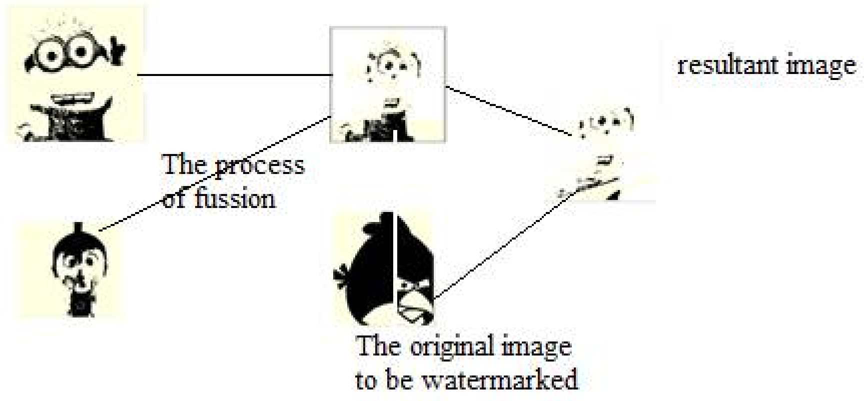


Fig 2: Block diagram for watermark embedding

C.*Watermark Extraction*

Watermark extraction assumes to have some original data. For extracting the data, backward embedding process is carried out. In this system, the embedding is done using arithmetic blend extension .for extraction the reverse process of that method is carried out.

D.*Watermark Authentication*

Authentication is for confirming the truth of an attribute of a single piece of data. User can give access to secure systems based on user credentials that imply authenticity.

IV. QUALITY OF THE WATERMARKED IMAGE

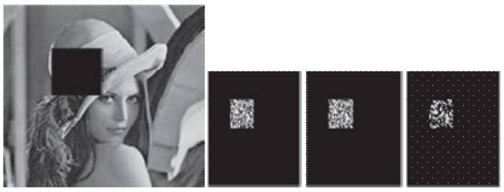
The value of the watermarked image can be obtained by the following methods

1. Mean Squared Error(MSE)
2. Peak Signal to Noise Ratio(PSNR)

1.*Mean Squared Error*

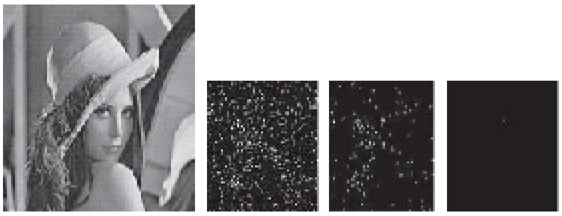
The mean squared error (MSE) is derived in the embedding process. Since there is crudely an equal spreading of all values in the estimate subband. we undertake that the unique wavelet coefficients in the approximation subband are regularly scattered over the series of [kq, (k + 1)q] for k ϵ Z. When the parity of the quantization result of theunique wavelet coefficient LLi(x, y) equals the inserted watermark bit Wi, Li (x, y) is changed to the lower-bound kq, and the MSE cause by this quantization is:

$$\mathrm{MSE} = \frac{1}{q}\int_0^q \tau^2 d\tau = \frac{q2}{3} \text{ --------------------- (1)}$$



(a)M1= 0.0325 and M2= 0.8218

Fig 3: Maliciously attacked watermarked image



(b)M1= 0.0542 and M2= 0

Fig 4: 70% JPEG compressed watermarked image

MSE of embedding p watermark bits in the block based wavelet domain is:
MSE $^{=}$ ________$^{\times}$ ------------------- (2)
× ×

2. *Peak Signal to Noise Ratio*

Peak signal-to-noise ratio, frequently shortened as PSNR, is an engineering term for the ratio between the maximum possible control of a signal and the control of corrupting noise that affects the fidelity of its representation. Because many signals have a actual varied active range, PSNR is typically expressed in terms of the logarithmic decibel scale. PSNR is utmost normally used to amount the value of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the unique data, and the noise is the error announced by compression. PSNR is an estimate to human perception of reconstruction quality. While a developed PSNR commonly shows that the reconstruction is of higher value, in various cases it may not. Therefore the PSNR value of watermarked image is:

$$\mathrm{PSNR} = 20\log\left(\frac{255\times bs}{q}\sqrt{3}\right) \text{ ------------------ (3)}$$

V.TAMPERING DETECTION SENSITIVITY

The tampering detection sensitivity of our project is determined by the quantizer. The fault map seizures the deviations in the quantization results and kinds the tampering obvious for k 2 Z in the following two cases: (1)

(1) The wavelet coefficient LLi'(x, y) of the watermarked picture is 2kq and the operation causes a shift of LLi' (x, y) in the range of [(0.5 + 2k) q, (1.5 + 2k) q).

(2) The wavelet coefficient LLi'(x, y) of the watermarked picture is 2kq + q and the operation causes a shift of LLi'(x, y) in the range of [(1.5 + 2k) q, (2.5 + 2k) q).

VI.ROBUSTNESS TO JPEG LOSSY COMPRESSION AND JPEG2000 LOSSY COMPRESSION ATTACKS

By performing two kinds of compression, namely, conventional JPEG lossy compression .our scheme is also achieves lower than the threshold value of 0.2418 for MI’s for JPEG quality factors down to 50%. All these indicate that our scheme is additional tough in categorizing a watermarked image beneath JPEG compressions of at least 50% quality factor as true and categorizing a watermarked image beneath JPEG compression of a quality factor reaching from 10% to 50% as parenthetically slanted. Our new results on 200 watermarked images also check the above indication. To calculate the robustness of our planned scheme to JPEG2000 lossy compression attacks using quality factors of 1000% down to 100% with reducing step size of 100% and their equal JPEG compression attacks using quality factors of 100% down to 10% with a reducing step size of 10%.

VII.FRAGILENESS TO VARIOUS MALICIOUS ATTACKS

By performing various malicious attacks on 200 watermarked images to demonstrate the efficiency of our planned scheme in focusing the meanly tampered regions. To this end, we practical three kinds of genuine change on the watermarked image by using Photoshop to addition an external object, change the right eye, and eradicate the object (white and grey wavy decoration) on the lower right. The meanly argued image was then saved as a JPG image using the default compression setting. By closing that our scheme detects all three spitefully attacked watermarked image as maliciously tampered and acceptably focusses their tampered regions

VIII.DETECTION STATISTICS UNDER DIFFERENT SIMULATED ATTACKS

Lastly, we calculate the performance of our proposed system, the different of our proposed system in the spatial domain and four peer system under two PSNR values (e.g., image blurring, Gaussian low-pass filtering , median filtering , salt and pepper noise , JPEG compression , JPEG 2000 compression and substitution) and each specific group of simulated attacks, respectively. For the replacement attacks, we executed each of the three kinds of block substitution tracked by 80% JPEG compression 50 times on all of the 200 watermarked images.

IX.CONCLUSION

We proposed an image watermarking system for image content verification, which advance the robustness of the watermarked image .Our system can be useful to any visible media (like images or video). This system will be measured as one of the hopeful systems for multimedia authentication. Our development work includes studying the tampering detection sensibility when an image size varies, addressing geometric attack issues, and testing more images of various types.

REFERENCES

[1] D.M. Thodi, J.J. Rodriguez, Reversible watermarking by prediction-error expansion, in: Proceedings of the 2004 Southwest Symposium on Image Analysis and Interpretation, 2004, pp. 21–25.
[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Syst. J., vol. 35, no. 3, pp. 313–336, 1996.
[3] H. Luo, F.X. Yu, H. Chen, Z.L. Huang, H. Li, P.H. Wang, Reversible data hiding based on block median preservation, Information Sciences 181 (2) (2011) 308–328.
[4] D. M. Thodi and J. J. Rodriquez, “Prediction-error-based reversible watermarking,” in Proc. IEEE Conf. Image Processing, Oct. 2004, pp. 1549–1552
[5] J. Tian, Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems for Video Technology 13 (8) (2003) 890– 896.
[6] J. Tian, “Wavelet-based reversible watermarking for authentication,” in Security and Watermarking of Multimedia Contents IV—Proc. SPIE, E. J. Delp III and P. W. Wong, Eds., Jan. 2002, vol. 4675, pp. 679–690
[7] D.M. Thodi, J.J. Rodriguez, Expansion embedding techniques for reversible watermarking, IEEE Transaction on Image Processing 16 (3) (2007) 721–730.
[8] Dual Protection of JPEG Images based on Informed Embedding and Two Stage Watermark Extraction Technique ,Wen-Ning Lin ,Member , IEEE , Guo-Shiang Lin, and Sheng – Lung Cheng.