IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 10 (October. 2018), ||V (III) || PP 01-04

A Novel Scheme for Multimedia Content Protection by Biometric Encryption Watermarking Method

Shameem kappan[1], Dr. Muhamed Ilyas[2]. P, Dr. R. Vijayakumar[3]
Research Scholar, School of Computer Sciences, Mahatma Gandhi University Kottayam, Kerala, India
Principal, Sullamussalam Science. College, Areekode, Kerala, India
Professor, School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala, India.
Corresponding Author: Shameem kappan

Abstract: Multimedia content protection has become one of the most important and interesting research area. We present a multimedia content protection by utilizing both biometric and digital watermarking. The finger print, face and signature biometric feature of the owner is used to generate the watermark. We include these three different water mark on the host image by partitioning row wise or column wise and then embedding the watermark on it. Our scheme includes 2-D Single Level Discrete Hear Wavelet transform for image compression and Single value decomposition for embedding and extraction of the watermarks. Sometime any ownership dispute on the host image, the watermark i.e., the fingerprint, face and signature is extracted from the watermarked image and related to the biometrics of person claiming the ownership. If they match, the claiming person is the real owner of the host image.

Keywords: Digital Water marking, Biometrics, Digital Right Management[DRM], Single Level Discrete Haar Wavelet Transform[DWT], Singular value decomposition[SVD].

Date of Submission: 10-10-2018 Date of acceptance: 26-10-2018

I. INTRODUCTION

The digital copy right problem has been gaining important in the recent years due to proliferation digital technology. Piracy other copy right violation regarding digital multimedia content represent a significant problem for legal content owners and content distributors. (F. Hartunget al., 1999). Hence the protection of intellectual property right for multimedia content, often referred to as the digital right management [DRM] for multimedia, (Fred Von Lohmann, 2005) recently started receiving a considerable amount of interest.

Recently several DRM solutions has been proposed which makes use of and digital watermarking techniques (Scott Carver et al., 2001). The most vital function of DRM system is the copyright protection. The copy restriction such as permitting no or one or several unlimited copies of the multimedia data, and without right to produce copies of these can be enforced by DRM system (E.T. Lin et al., 2005). DRM consists of certain techniques which include encryption, digital water marking, finger printing, traitor tracing, authentication, key management and revocation (Ian Kerr, 2007). The objective of digital watermarking is to embed small amount of secret information, ie, the watermark into the host digital production like the image and audio, thus facilitating the extraction at the later stage for the purposes of copyright assertion, authentication and content integrity verification. (HuainSiChan-TsunLi, 2005). Digital watermarking techniques can have utilized to protect theintellectual property right of the data by embedding the proprietary information, such as company logo and password in the host data (G.Voyatsiz et al., 1999). Face recognition is important for to recognize an individual, find the best match by matching the input face image with the face image in the training data set. It is used to verify a persons claimed identity or identify a person. (M.Vikas,K et al., 2012,Y. T Xiao et al., 2006). Facerecognition plays an important role in our daily life for theidentification and authentication purpose [Fincy Francis et al., Mohammed Hasan et al., 2013). Handwritten signature is behavioral trait and can be used for person identification purpose. There are two types of identification modes available, online and offline mode. In the proposed scheme, we use watermarking and biometrics to protect the digital contents. In this paper, we have focused on the prevention of disputes that arise out of ownership claim on multimedia digital images and novel and efficient scheme to deal with it has been developed. In future biometric will play a vital role in security (John Chirillo, Scott Blaul). Finally, if any ownership dispute arises, biometric help to solves the situation because of the insertion of biometric feature as the watermark in the proposed scheme, Extracted watermark image are compared with test image using correlation analysis.2D Single Level Discrete Haar Wavelet Transform used for image compression transformation and Singular Value Decomposition embed the watermark to host image.

The rest of the paper is organized as follows; Section 2 presents a brief review of some of the works available in the literature of biometric and water marking. In section 3 proposed scheme for digital right management of images using biometrics is presented in details. Section4 describe the result and conclusions are summed up in section 5.

II. RELATED WORKS

The study of watermarking on images employed in the automatic personal identification technology based fingerprints was proposed by Minerva M Yeung (Minerva M Yeung and SharatPankanti). They investigated the effect of watermarking fingerprint images on the identification and extraction accuracy with the aid of invisible fragile watermarking technique for image verification application on a particular finger print recognition system.

Mohamed Mostafa abd Allah proposed a methodology for recognition of a finger print with the aid of artificial Neural Networks (Mohd Mostafa Abd Allah, 2005). A clustering algorithm was employed by them for the identification of similar feature groups from template images generated from the same finger and a cluster core set was created. A multimedia content protection scheme that worked on biometric data of the users and layered encryption /decryption scheme were presented by UmutUludag(UmutUldag et al.).

Tuan Hoang proposed a remote multimodal biometric authentication frame work that worked on basis of fragile watermarking for the transmission of multi-biometrics over networks to server for authentication (Tuan Hoang et al.,2008). Their proposed frame work improves and security and brings down bandwidth.

A new face recognition method based on opposition based PSO with SVM is introduced by Muhammed Hassan and SNH Abdulla (Mohammed Hasan et al., 2013).

III. MULTIMEDIA CONTENT PROTECTION BY BIOMETRIC ENCRYPTION WATERMARKING METHOD

In our methodology, a novel scheme of multimedia content protection by Biometric encrypting water making method is proposed. we have used several standard images, for example ‘cameraman’, ‘lena’, ‘mandril’ and ‘peppers’ for our experiments as host images. For watermarking, we have used three different biometrics for embedding i.e., fingerprint, face and signature from FVC, AT&T and CEDAR datasets respectively. Both host image and biometric watermarks are converted to grayscale by ignoring huge and saturation information in the image and maintaining only intensity information. The intensity is estimated by the mean of red, green and blue components of each pixel. In case of fingerprint and signature, the images are negated to eliminate whitening of the host image, as it contains more background pixels than the original content.

We have included three different watermarks on the host images by partitioning the host images into three equal parts and then embedding one on the other, this will ensure better watermarking and identification accuracy. The host images are partitioned into three equal parts row-wise orcolumn-wise on the basis of its divisibilityinto three equal parts. The host image is resized if needed by ensuring minimum increase in row size or column size

III.a Single Level Discrete Haar Wavelet Transform

Our watermarking scheme includes 2-D Single Level Discrete Haar Wavelet Transform(DWT) and Singular Value Decomposition(SVD). The discrete wavelet transformation is used for image compression transformation. By wavelet transformation we decompose our image into a set of basic functions known as wavelets. Wavelets are obtained from a single prototype wavelet called mother wavelet. By 2-D DWT, we mean DWT scheme along row-wise and then again performing DWT along column-wise. By incorporating DWT for watermarking, we desire to eliminate highly correlated redundant pixel values in the spatial domain by transforming it into frequency domain. Haar transform is the simplest form of wavelet transform, unlike other transforms, it is not continuous. The Haar Wavelet Transformation is a simple form of compression which involves averaging and differencing terms, storing detail coefficients, eliminating data, and reconstructing the matrix such that the resulting matrix is similar to the initial matrix.

The Haar wavelet's mother wavelet function Ψ(t) can be computed using:

$$\Psi(\mathrm{t}) = \begin{cases} 1 & 0 \le t < \frac{1}{2}, \\ -1 & \frac{1}{2} \le t < 1, \\ 0 & otherwise \end{cases}$$

The scaling function of Haar Transform $\varphi(t)$is given by:

$$\varphi(t) = \begin{cases} 1 & 0 \le t < 1, \\ 0 & otherwise \end{cases}$$

III.b Embedding the three water mark in to Host image

The Singular Value Decomposition (SVD) is used to embed our watermarks to the host image due to its reversible property. The singular-value decomposition of an MXN reall or complex matrix M is a factorization of the form USV^T, where U is an MXM real or complex unitary matrix, S is a MXN rectangular diagonal matrix with non-negative real numbers on the diagonal, and V is an NXN real or complex unitary matrix. The diagonal entries of S are known as the singular values of M. The columns of U and the columns of V are called the left-singular vectors and right-singular vectors, respectively. These values can be obtained using following algorithm.

i. Compute square roots of the Eigen values of M.
ii. Arrange above values in decreasing order to obtain S.
iii. Eigen vectors of MM^T and M^TM gives U and V respectively.

Once we carry out DWT, we will have an approximation coefficient, it is the low pass representation of the signal. The approximation coefficient of the host part and biometric image are passed on to SVD routine separately. The singular values of the biometric is multiplied with a constant alpha and then both singular values are added together. Then the approximation coefficient is reconstructed using left singular values and right singular values of host part accompanied with new singular values.

$$M_{host} = U_{host} S_{host} V_{host}^T$$
$$M_{mark} = U_{mark} S_{mark} V_{mark}^T$$
$$S_{host} = S_{host} + (\propto S_{mark})$$
$$M_{host} = U_{mark} S_{host} V_{mark}^T$$

Inverse DWT is performed and the parts are obtained with hidden biometric watermarks. All the three parts are concatenated to acquire our watermarked host image. The Peak Signal-to-Noise Ratio (PSNR) is used to measure the performance of the watermarking algorithm.

III.c Extraction of water mark from Host image

For extracting watermark from the watermarked image, we follow the same procedure of dividing into three partitions as these three partition contains our three different biometric traits. The approximate coefficient using DWT is found from each part and SVD is performed. The left-singular vectors U and right-singular vectors V of the host image obtained during the singular decomposition of original image is used with the present singular value S to reconstruct the biometric from the watermarked image.

$$M_{mark} = U_{host} S_{water\ host} V_{host}^T$$

The extracted watermark images are compared with original watermark image of the author using correlation analysis. For this, first both images are resized to 100x100 matrix and then the correlation C of both images are computed. If the correlation value is greater than 0.8 then it is accepted as original watermark image.

$$C = \frac{\left(\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})\right)}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A})^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2)}}$$

Where $\bar{A}$ and $\bar{B}$ are mean of respective matrix elements.

III.d Verification of owner ship

Verification of ownership is the assessing the rightful owner of the digital data. If some ownership dispute arises correlation analysis is used for finding the actual owner of the image.

The process is extracted watermark images are compared with test images using correlation analysis. First both images are resized to 100x100 matrix. Then correlation of both images are computed. If the correlation value is greater than 0.8 then it is accepted as the original watermark image and the person is the actual owner of the image.

IV. EXPIRIMENTAL RESULT

For experimentation purpose, we have used some of the well-known images as our host image. We have implemented our proposed scheme in MATLAB 16. We have embedding three different biometric watermarks into three different parts of the host image. So PSNR value of each part as well as the total value is computed. We have watermarked first part with fingerprint, second with face and the final part with signature. We have used standard dataset FVC for fingerprint, AT&T for face and CEDAR for signature. To compute PSNR, we will use first biometric from each database to all the host images to maintain fairness in the results.

$$PSNR = 10 \log_{10}(peakvalue^2/MSE)$$

The peak value of the grayscale image is 255 and MSE is the Mean Squared Error.

Image Name (512x512)	PSNR Value for fingerprint watermark	PSNR Value for face watermark	PSNR Value for signature watermark	Total PSNR(dB)
cameraman	26.45	28.20	33.15	28.47

lena	27.97	24.96	24.65	25.62
mandril	22.53	19.53	22.21	21.20
peppers	32.61	31.25	29.17	30.77

V. CONCLUSION

A Digital Right Management system need to be capable of providing content protection against illegal access to the digital content, provided access to only person those with appropriate authorization. Watermarking techniques are being used for this purpose. The embedded watermark data can be easily hacked by the hacker and thus result as a threat to protection of digital content. To solve this security, issue in protecting the right of digital content, we have presented a method, watermarking with three biometrics to enhance the security of multimedia data protection. In the proposed scheme images of the thump, face and signature of the owner are embedded on the host image as water marking. The watermark embedding and extraction wereperformed in DWT-SVD method. When the ownership dispute arises, the embedded image serves as a proof for the rightful ownership verification of the image.

REFERENCE

[1]. F. Hartung and M. Kutter, (1999). Multimedia water marking Techniques.Proc. IEEE, Vol 87, No.7, July, pp.1079-1107.

[2]. Fred Von Lohmann. (2005). Fair use and Digital Right Managements: Preliminary thought on the (Irreconcilable?) Tension between them.Proc. Of Electronic Frontier Foundation. March.

[3]. Scott Carver, Stefan Katsenbeizer. (2001).Copyright protection protocol based on asymmetric watermarking: The ticket concept.Communication and Multimedia Security issue of new century, pp.159-170.

[4]. E.T. Lin, A.M. Eskicioglu, E.J. Delp. (2005). Advances in digital video content protection.IEEE: Special issue on Advances in video coding and delivery, pp.171-183.

[5]. Ian Kerr. (2007). Hacking @privacy: Why we need protection from technologies that protect copyright. Proc. Conference of privacy.

[6]. HuainSiChan-TsunLi. (2005). Copyright protection in virtual communities through digital watermarking. Idea group publishing.

[7]. G.Voyatsiz and I Petes. (1999). The use of watermark in the protection of digital multimedia products.IEEE Proceedings, Vol. 87, No. 7, pp.1197-1207.

[8]. John Chirillo, Scott Blaul. Implementing Biometric Security, John Wiley Publishers

[9]. Minerva M Yeung and SharatPankanti. Verification Watermark on Finger Print Recognition and Retrieval.SPIE Proceedings Vol. 3657.

[10]. Mohd Mostafa Abd Allah. (2005). Artificial Neural Network Based Finger print authentication with Clusters Algorithm.Proc. of Informetica, pp.303-307.

[11]. UmutUldag and Anil.Kjain. Multimedia content protection via Biometrics based encryption.Proc. International conf. on Multimedia and Expo, Vol.3.

[12]. Tuan Hoang, Dharmendra Sharma.(2008). Remote multimodal Biometric Authentication using Bit priority based Fragile Watermarking.Proc. International conf. on pattern recognition.

[13]. Alexander Sverdlov, Scott Dexter, Ahmat M Escigoglu. (2005). Robust DCT_SVD domain image watermarking for copy right protection: embedding data in all frequencies.Proc. Annual European signal processing Conference.

[14]. L. Lam, S. W. Lee and C Y Seun. (1992). Thinning Methodologies –a comprehensive survey. IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 14.

[15]. M.Vikas,K, Sushila, A Sunnita, KS Vinay. (2012). DCT-Based Reduced face for face recognition.International Journal of Information Technology and Knowledge Management, X5(1), pp.97-100.

[16]. Y. T Xiao, C Songakan, H.Z.Zhi, Z.Fuyan. (2006). Face recognition from a single image per person A Survey.Pattern recognition 39(9) pp 1725-1745.

[17]. Fincy Francis, AparnaMS,Anitta Vincent. Biometric Online Signature Verification.IOSR-JECE, pp. 82-89

[18]. Mohammed Hasan, SNHS Abdulla, Zulaiha Ali Otman. (2013). Face Recognition Based on Opposition Particle Swarm Optimization and Support Vector Machine, IEEE international conference(ICSIPA).

Shameem kappan. " A Novel Scheme for Multimedia Content Protection by Biometric Encryption Watermarking Method" IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 10, 2018, pp. 01-04.