Authenticity For Protecting Biometric Data: Facial Template and Iris Detection

Harmanpreet Kaur[1] Shifali Singla[2]
[1]M.Tech Student [2]Assistant Professor
[1]Department of Computer engineering
[1,2]YCoE, Talwandi Sabo

Abstract— A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Digital watermarks can be used to verify the authenticity or integrity of the original signal or to show the identity of its owners. The conventional digital watermarking schemes uses an arbitrary digital pattern as a watermark which has limitations in providing ownership of watermarking. The proposed technique of watermarking include combined watermark embedding and extraction using SVD (Singular Value Decomposition), DWT (Discrete Wavelet Transform) and DCT (Discrete Cosine Transform). The proposed technique is based on the face detection and iris detection for authenticity and ownership of original data. This proposed technique will give us the better results of security and better quality of data without any loss during transmission of data.

Key words: Biometric Data, Facial Template, Iris Detection, DWT, DCT.

I. INTRODUCTION

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. The existing digital watermarking schemes use a digital pattern like pseudorandom number sequence, a logo image or a digital signature as the watermark. Content authentication and ownership issues of multimedia data such as images is becoming more and more important in the fields of law enforcement, digital right management, medical imaging etc. In the recent times the production, distribution, and use of digital media has become very popular. Although all these products have the advantages of high quality, ease of modification, and quality duplication, they introduce the problems of copyright protection issues because they can be easily copied and altered. In this condition, there is a strong requirement for techniques to protect the copyright of the original media to prevent its unauthorized duplication. One potential solution to address this problem involves inserting an invisible digital pattern to a host signal to prove its copyright ownership. These digital patterns which are used for embedding are known as digital watermarks. The authentication process is done by biometrics such as fingerprints, face templates etc. The proposed technique involved authentication and extraction of watermarking by face recognization and iris detection to verify the identity of individual. These techniques provide better security and better quality of watermarking .

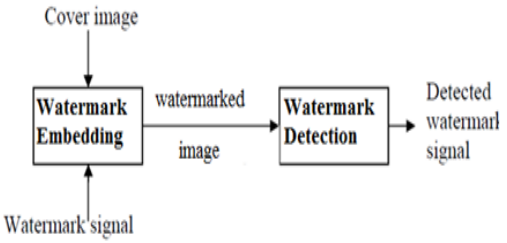

Fig. 1: Generic Watermarking Scheme[4]

This paper is organized as follows. In section II related work for this research is defined. Section III gives the Proposed Techniques of watermark embedding. Section IV gives the Authentication and Extraction of Watermark Section V gives the parameter to evaluate. Finally, Section 6 gives the conclusion of the work.

II. .RELATED WORK

Cui-ling JIANG et al., [1] have presents the cover image is divided into non-overlapping blocks of 16×16 pixels instead of traditional dividing cover-image into 8×8 blocks and the DCT is used to transform each block. The DCT coefficients are quantized and embedded the secret messages. The method has the larger steganography capacity and better stego-image quality than the other methods. Hui-Yu Huang [2] proposes a technique lossless data-hiding method for a DWT. Using the quantization factors for DWT, our proposed approach can offer high hiding capacity and preserve the image quality of stego-images. The original image can be recovered losslessly when the secret data had been extracted from stego-images.

The least-significant bit (LSB) [9] insertion method is the most common and easiest method for embedding messages in an image. An image steganographic model is proposed that is based on variable-six LSB insertion to maximize the embedding capacity while maintaining image fidelity. For each pixel of a grey-scale image, at least four bits can be used for message embedding. Three components arc provided to achieve the goal. First, according to contrast and luminance characteristics, the capacity evaluation is provided to estimate the maximum embedding capacity of each pixel. From literature review digital data hiding in cover image using wavelet gives the good results as compared to other methods.

III. PROPOSED TECHNIQUE

According to the domain in which watermark is inserted, these techniques are divided into two broad categories[3]-:

- Spatial Domain method
- Frequency Domain method

Embedding the watermark into spatial domain component of the original is straight forward method. LSB scheme is one of the example from spatial domain which modifies lower order bits of cover image to embed the watermark. It has the advantage of low complexity and easy implementation but problem with this scheme is low security, because it is possible to remove the watermarked image easily by setting all LSBs or pixels to zero. Frequency domain schemes have become popular watermarking algorithms based on frequency domain. These are more persistent to general image processing than spatial domain algorithm. DFT, DCT and DWT are some algorithms from this category.

The proposed technique of watermarking includes following algorithms:-

- SVD (Singluar Value Decomposition)
- DWT (Discrete Wavelet Transform)
- DCT (Discrete Cosine Transform)

A. SINGULAR VALUE DECOMPOSITION:

In linear algebra, the singular value decomposition (SVD) is a factorization of a real or complex matrix, with several applications in signal processing [2]. The SVD can be seen as a generalization of the spectral theorem to arbitrary, not necessarily square matrices. The basic idea behind SVD is taking high dimensional highly variable set of data points and reducing it to a lower dimensional space that exposes the substructure of the original data more clearly. Suppose M is an m-by-n matrix. Then there exists a factorization for M of the form $M=U\ \Sigma V^T$ where, U is an m-by-m unitary matrix, a diagonal matrix Σ is m-by-n with non-negative numbers in descending order and V^T denotes the conjugate transpose of V, an n-by-n unitary matrix. Such a factorization is called a singular value decomposition of M.

A matrix is orthogonal if $U^TU=V^TV=I$

- The matrix V thus contains a set of orthonormal input vector directions for the matrix M.
- The matrix U thus contains a set of orthonormal output basis vector directions for the matrix M.
- The matrix Σ contains the singular values, which can be thought of as scalar gain controls by which each corresponding input is multiplied to give a corresponding output.

B. B. DCT DOMAIN WATERMARKING:

Discrete Cosine Transform (DCT) method is used to convert time domain signal into frequency domain signal. Using DCT, an image is easily split into pseudo frequency bands and in this work watermark is inserted into middle band frequencies because as we discussed in all frequency domain watermarking schemes, there is a conflict between robustness and transparency.

C. C. DWT DOMAIN WATERMARKING:

This watermarking method is focusing on its embedding strength would provide useful insight in how to improve its performance. The performances measured include robustness, imperceptibility and computational cost.DWT decomposes an image into a low-pass sub band and three high- pass sub bands. In this study, this method embeds a watermark in high-pass (or higher frequency) band of the DWT domain. This is due to the good imperceptibility provided by high-pass band. To reconstruct an image, an inverse DWT is used after modification has been made by using singular values of SVD of watermark[3].

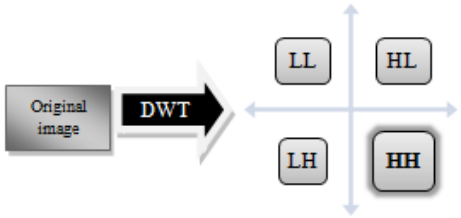

Fig. 2: Decomposition of Image using DWT [4]

D. SVD- DWT-DCT BASED WATERMARKING:

This method utilizes the wavelet coefficients of the cover image to embed the watermark. Any of the three high frequency sub bands of wavelet coefficients can be used to watermark the image. The DCT coefficients of the wavelet coefficients are calculated and singular values decomposed. The singular values of the cover image and watermark are added to form the modified singular values of the watermarked image. Then the inverse DCT transform is applied followed by the inverse DWT. This is the algorithm that clubs the properties of SVD, DCT and DWT. Watermark embedded using this algorithm is highly imperceptible. This scheme is robust against all sorts of attacks. It has very high data hiding capacity. The new method was found to satisfy all the requisites of an ideal watermarking scheme such as imperceptibility or fidelity, robustness and good capacity.

IV. AUTHENTICATION AND EXTRACTION OF WATERMARK

The authentication process includes various biometric security parameters. In our proposed research work the first step of authentication is done by face recognization. After the face recognization iris detection is performed for identification. when both the identification using face and iris detection is performed ,the original and watermark images are extracted by performing extraction algorithm. These type of identification method provide better security to original data without any loss. This identification process required databases for face and iris detection which includes the face and iris templates for matching process. This proposed technique of authenticity adresses the limitation of copyright protection.

Figures used for proposed technique

Fig. 3: Original Image lena.jpg [3]

Fig. 4: Watermark Image cameraman.jpg [3]

V. PARAMETER TO EVALUATE

Peak Signal to Noise Ratio

For performance evaluation, the visual quality of watermarked image is measured using the Peak Signal to Noise Ratio, which is defined in Equation(1)

$$PSNR = 10\log\left(\frac{255^2}{\text{MSE}}\right) \qquad (1)$$

Where MSE is mean square error defined in Equation (2)

$$\text{MSE} = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{[OI(i,j)-D(i,j)]^2}{MXN} \qquad (2)$$

Where OI and DI denote the gray-level values between original and watermarked image; M and N are the height and width of the image, respectively[3].

V. CONCLUSION

We proposed a new watermarking scheme and a biometric authenticity for data security using face template and iris detection which provide a complete algorithm that embeds and extracts watermark information effectively. It has been confirmed that the proposed watermarking method is able to extract the embedded message watermark from the watermarked images .The embedded watermark is extracted by authentication of owner's facial template and iris detection.This technique enhance the security of data using biometric identification and gives us better quality of original and watermark data.

REFERENCES

[1] Cui-ling JIANG "A Steganographic Method based on the JPEG Digital images" Institute of Information, East China University of Science and Technology, 2011.
[2] Hui-Yu Huang & Shih-Hsu Chang "A lossless data hiding based on discrete Haar wavelet transform", 10th IEEE International Conference on Computer and Information Technology, 2010
[3] Pallavi Patil, D.S. Bormane," DWT Based Invisible Watermarking Technique for Digital Images" Volume 2,April 2013.
[4] Malay Kishore Dutta, Anushikha Singh, & Tanveer A Zia," An Efficient and Secure Digital Image Watermarking Using Features From Iris Image" IEEE 2013.
[5] Cameron Whitelam, Nnamdi Osia and Thirimachos Bourlai," Securing Multimodal Biometric Data through Watermarking and Steganography" IEEE 2013.
[6] Mrs. Sunita Roy and Mr. Susanta Podder,"Face detection and its applications" ,ijreat,Volume 1, May 2013.
[7] Gargi Amoli, Nitin Thapliyal, Nidhi Sethi, " Iris Preprocessing", ijarcsse., Volume 2, June 2012.
[8] Sheeba Jeya Sophia S. and Veluchamy S., " Security System Based on Iris Recognition" isca,vol 3 ,March 2013.
[9] Y. K. Lee and L.H. Chen, "High capacity image steganographic model", Vision, Image and Signal Processing, IEEE Proceedings, 2000
[10] KevinW. Bowyer, Karen P. Hollingsworth, and Patrick J. Flynn, "A Survey of Iris Biometrics Research" Springer-Verlag London ,2013.
[11]Rolibansal,PritiSehgal,PunamBedi,"Intelligent wavelet domain watermarking of fingerprint images", IEEE, 2012.
[12] Mohamed Ouslim, AhmedSabri, HassanMouhadjer, "Securing biometric data by combining watermarking and cryptography", Sciencedirect, 2013.

