



Study on Watermarking Approaches on Biometric Images

¹Neeraj, ²Sunita

¹Student, M.Tech, ²Asstt. Professor,
Deptt. of Computer Sc., Baba Mast Nath Engg. College
Rohtak, Haryana, India

Abstract: To obtain the information security and information authentication one of effective approach is watermarking. In this approach, the data is hide behind some multimedia objects. One of such effective watermarking concept is provided by Biometric Image watermarking. In this work, an analysis on DCT and DWT based watermarking approaches is defined to perform Biometric Image watermarking. In this paper, the issues and challenges associated with watermarking process are also discussed.

Keywords: Biometric Image Watermarking, DWT, DCT, Noisy, Compression

I. INTRODUCTION

To protect the Biometric Image and the Copy Protection Technical Working Group (CPTWG), an ad hoc group consisting of the Motion Picture Association of America, the Consumer Electronics Manufacturers Association, and members of the computer industry, examine the digital Biometric Image protection in the form of Biometric Image watermarking. The system was designed basically for the DVD copyright protection. The Biometric Image watermarking provides the Biometric Image protection with better robustness and transparency. In this watermarking system, the watermark conveys the information about the copying authority like copy once, copy never, copy freely etc. The another advantage of this mechanism is the cost effectiveness. It provides the higher security and reliability in terms of low false positive rate. This Biometric Image watermarking was defined with MPEG decoder. The watermark is embedded within the drive that makes it sure that watermark will stay till the multimedia content is available in the DVD. But to include some more features such as cryptography and the authentication over the watermark contents, the application based watermarking come into the picture. This application oriented watermarking scheme gives more flexibility to extend the application as well as the methodology.

The extension to this Biometric Image marking approach is the inclusion of second watermark. This second watermark scheme is inexpensive and basically used for the compressed Biometric Images. The another watermarking approach is based on tickets that represents a cryptographic counter defined by hash key and this counter is incremented each time the Biometric Image pass to the recorder. The another scheme adopted by Biometric Image watermarking is the scene based watermarking. This scheme basically separate the static and dynamic areas of the Biometric Image frames by using wavelet decomposition. Now these static areas are used to store the watermark objects [6].

The another issue associated with Biometric Image watermarking is the compressed Biometric Image formats. These compressed Biometric Image formats having the compressed bit streams so that full length decoding process cannot be implemented here. These kinds of Biometric Image formats increase the complexity as well as delay while performing the watermarking [6].

A. Requirements of Biometric Image Watermarking

Some of the requirements of watermarking are discussed in earlier section. But along with this, the additional requirements of Biometric Image watermarking is given as [7]

(i) Compressed Data Procassing

In normal case, the Biometric Image watermarking system must be operated under the compressed domain because most of the avaiable Biometric Image formats are itself in compressed forms. To achieve the robustness, it is required for a watermarking approach to be feasible in compressed, recompressed and decompressed forms.

(ii) Fast Embedding/Detection

Generally, the size of Biometric Image data is quite large so that a Biometric Image watermarking algorithm must be fast enough to process the Biometric Image and to minimize the process delay.

(iii) Blind Detection

In case of Biometric Image watermarking, there is no availability of original Biometric Image while performing the watermark detection. Because of this it is important for Biometric Image watermarking to perform the detection process by analyzing the Biometric Image sequences. But the detection process, can have the watermarked object to perform the detection.

B. Watermarking Perspectives

The perceptivity of the watermark actually defines the need of the user or the actual requirement of user. These requirements can be crystal clear, if we get the features of these perspectives. The features of these two classes are listed in Table 2.

Table 2: Perceptive based Classification

	Visible Watermarking
Feature	• Overwrite the Existing media contents • Cannot remove watermarks completely • Used for logos or the trademarks
Advantage	• Direct Confirmation • Comparatively Fast
Disadvantage	• Fragility to Attack • Degrade Quality
	Invisible Watermarking
Features	• Most Commonly used • Necessary for commercial authentication
Advantages	• Not Degrade the contents
Disadvantages	• Can be modified

II. LITERATURE REVIEW

C. K. Chan *et al.* [1] presented a data hiding scheme by simple LSB substitution is proposed. By applying an optimal pixel adjustment process to the stego-Biometric Image obtained by the simple LSB substitution method, the Biometric Image quality of the stego-Biometric Image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-Biometric Image and the cover-Biometric Image is derived. Experimental results show that the stego Biometric Image is visually indistinguishable from the original cover-Biometric Image. Sanjeev Manchanda *et. al* [2] stated that steganography is the science of hiding information in media based data. They present random numbers logic based steganographic methods and layout management schemes for hiding data/Biometric Image into Biometric Image(s). These methods and schemes can be customized according to the requirements of the users and the characteristics of data/Biometric Images. These methods are secure enough to meet the requirements of the users and user can play significant role in selection and development of these methods. Methods can be chosen randomly and implemented dynamically based on inputs, user choices as well as outputs. Experimental results are given to demonstrate the performance of the proposed methods. Xinpeng Zhang *et. al* [3] said that the pixel-value differencing (PVD) steganography can embed a large amount of secret bits into a still Biometric Image with high imperceptibility as it makes use of the characteristics of human vision sensitivity. However, a loophole exists in the PVD method. Unusual steps in the histogram of pixel differences reveal the presence of a secret message. An analyst can even estimate the length of hidden bits from the histogram. To enhance security, a modified scheme is proposed which avoids occurrence of the above-mentioned steps in the pixel difference histogram while preserving the advantage of low visual distortion of the PVD. The histogram-based steganalysis is therefore defeated. H.-C. Wu, N.-I. Wu *et. al* [5] proposed a method in order to improve the capacity of the hidden secret data and to provide an imperceptible stego-Biometric Image quality, a novel steganographic method based on least-significant-bit (LSB) replacement and pixel-value differencing (PVD) method is presented. First, a different value from two consecutive pixels by utilising the PVD method is obtained. A small difference value can be located on a smooth area and the large one is located on an edged area. In the smooth areas, the secret data is hidden into the cover Biometric Image by LSB method while using the PVD method in the edged areas. Because the range width is variable, and the area in which the secret data is concealed by LSB or PVD method are hard to guess, the security level is the same as that of a single using the PVD method of the proposed method. From the experimental results, compared with the PVD method being used alone, the proposed method can hide a much larger information and maintains a good visual quality of stego-Biometric Image. Hwang M.S. *et. al* [6] proposed that in a (t, n) threshold proxy signature scheme, the original signer delegates the power of signing messages to a designated proxy group of n members. Any t or more proxy

signers of the group can cooperatively issue a proxy signature on behalf of the original signer, but $(t-1)$ or less proxy signers cannot. Previously, all of the proposed threshold proxy signature schemes have been based on the discrete logarithm problem and do not satisfy all proxy requirements. In this paper, they propose a practical, efficient, and secure (t, n) threshold proxy signature scheme based on the RSA cryptosystem. Their scheme satisfies all proxy requirements and uses only a simple Lagrange formula to share the proxy signature key. Furthermore, their scheme requires only 5 percent of the computational overhead and 8 percent of the communicational overhead required in Kim's scheme.

Chen et. al [7] proposed a new Biometric Image cryptosystem to protect Biometric Image data. It encrypts the original Biometric Image into another virtual Biometric Image. Since both original and virtual Biometric Images are significant, this new cryptosystem can confuse illegal users. Besides the camouflage, this new cryptosystem has three other benefits. First, this cryptosystem is secure even if the illegal users know that the virtual Biometric Image is a camouflage. Second, this cryptosystem can compress Biometric Image data. Finally, this method is more efficient than a method that encrypts the entire Biometric Image directly. Fu, M.S et. al [8] said that in many printer and publishing applications, it is desirable to embed data in halftone Biometric Images. In this paper, they proposed some novel data hiding methods for halftone Biometric Images. For the situation in which only the halftone Biometric Image is available, they propose data hiding smart pair toggling (DHSPT) to hide data by forced complementary toggling at pseudo-random locations within a halftone Biometric Image. The complementary pixels are chosen to minimize the chance of forming visually undesirable clusters. Their experimental results suggest that DHSPT can hide a large amount of hidden data while maintaining good visual quality. For the situation in which the original multitone Biometric Image is available and the halftoning method is error diffusion, they propose the modified data hiding error diffusion (MDHED) that integrates the data hiding operation into the error diffusion process. In MDHED, the error due to the data hiding is diffused effectively to both past and future pixels. Their experimental results suggest that MDHED can give better visual quality than DHSPT. Both DHSPT and MDHED are computationally inexpensive.

III. WATERMARKING APPROACH

In this present work, a DWT and DCT based approach for Biometric Image Watermarking approach is presented. These approaches are most effectively used to perform effective information storage in image objects. The discussion on these two approaches is given here under

A. DCT

DCT is one of the important approaches that first separate the video frames in smaller parts and assign the weightage to these parts under the quality analysis. The concept of DCT is similar to the Fourier transformation so that the signal is identified under the spatial domain and the frequency analysis on these frames will be done effectively.

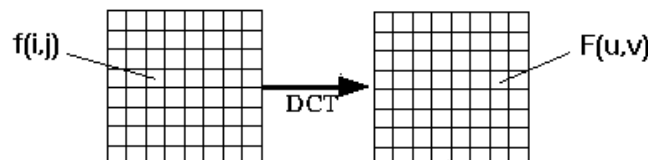


Figure 1: DCT Encoding

The basic process defined by DCT is given as under

- As the video frames is accepted by the DCT, it split the frame in smaller windows of size $n \times m$.
- Extract the intensity from different window forms at position (I, j)
- Define the coefficient for each row and column under the DCT coefficient matrix.
- The extraction of low frequency areas from the frame that will be used as the key area for storing the data over the image
- The compression will be performed effectively by neglecting the non visible areas so that no visible distortion will be done.
- Define the DCT array of integer so that the gray level scaling will be done.
- The matrix contents will be reterived under different formats such as horizontally, vertically, in zig-zag motion.

B. DWT

The DWT is one of the fundamental processes in the JPEG2000 image compression algorithm [4]. The DWT is a transform which can map a block of data in the spatial domain into the frequency domain. The DWT returns information about the localized frequencies in the data set. A two-dimensional (2D) DWT is used for images. The 2D DWT decomposes an image into four blocks, the approximation coefficients and three detail

coefficients. The details include the horizontal, vertical, and diagonal coefficients. The lower frequency (approximation) portion of the image can be preserved, while the higher frequency portions may be approximated more loosely without much visible quality loss. The DWT can be applied once to the image and then again to the coefficients which the first DWT produced. It can be visualized as an inverted treelike structure. The original image sits at the top. The first level DWT decomposes the image into four parts or branches, as previously mentioned. Each of those four parts can then have the DWT applied to them individually, splitting each into four distinct parts or branches [5].

IV. CONCLUSION

In this paper, an effective approach is defined to perform the Biometric Image watermarking using DCT and DWT based approaches. The paper has discussed the issues associated with watermarking along with approach specification.

References

- [1] C. K. Chan and L. M. Chen, "Hiding Data in Biometric Images by Simple LSB Substitution," *Pattern Recognition*, Vol. 37, Issue (3), pp. 469–474, 2004.
- [2] Sanjeev Manchanda, Mayank Dave and S. B. Singh, "Customized and Secure Biometric Image Steganography Through Random Numbers Logic", *Signal Processing: An International Journal*, Vol. 1, Issue (1), 2007.
- [3] Xinpeng Zhang, Shuozhong Wang, "Vulnerability of Pixel-Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security", *Pattern Recognition Letters*, Vol.25, pp. 331–339, 2004.
- [4] Rafael C. Gonzalez, Richard E. Woods, "Digital Biometric Image Processing" 2nd ed., 2002.
- [5] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang, M.S., "Biometric Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods. *IEE Proceedings – Vision Biometric Image and Signal Processing* Vol. 152, pp. 611–615, 2005.
- [6] Hwang M.S., Lu, E.J.L., and Lin, I.C., "A Practical (t, n) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem", *IEEE Trans. Knowl. Data Eng.*, Vol. 15, Issue (6), pp. 1552–1560, 2003.
- [7] Chen, T.S., Chang, C.C., and Hwang, M.S., "A Virtual Biometric Image Cryptosystem Based upon Vector Quantization", *IEEE Trans. Biometric Image Process.*, Vol. 7, Issue (10), pp. 1485–1488, 1998.
- [8] Fu, M.S., and Au, O.C., "Data Hiding Watermarking for Halftone Biometric Images", *IEEE Trans. Biometric Image Process.*, Vol. 11, Issue (4), pp. 477–484, 2002.
- [9] Tseng, Y.C., Chen, Y.Y., and Pan, H.K., "A Secure Data Hiding Scheme for Binary Biometric Images", *IEEE Trans. Commun.*, Vol. 50, pp. 1227–1231, 2002.
- [10] Tseng, Y.C., and Pan, H.K., "Data Hiding in 2-color Biometric Images", *IEEE Trans. Comput.*, Vol. 51, Issue (7), pp. 873–878, 2002.
- [11] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, "Adaptive Data Hiding in Edge Areas of Biometric Images with Spatial LSB Domain Systems." *IEEE Transactions on Information Forensics and Security*, Vol. 3, Issue (3), September 2008.
- [12] D. Artz, "Digital Steganographic: Hiding Data within Data," *IEEE Internet Comput.*, Vol. 5, Issue (3), pp. 75–80, May/Jun. 2001.
- [13] R. R. Anderson and F. A. P. Peticolas, "On the Limits of Steganography", *IEEE J. Sel. Areas Commun.*, Vol. 16, Issue (4), pp. 474–481, May 1998.
- [14] Chih-Chiang Lee, Hsien-ChuWu, Chwei-Shyong Tsai, Yen-Ping Chu, "Adaptive Lossless Steganographic Scheme with Centralized Difference Expansion", *Pattern Recognition* Vol. 41, pp. 2097 – 2106, 2008.
- [15] Martin Alvaro, Sapiro Guillermo and Seroussi Gadiel, "Is Biometric Image Steganography Natural?", *IEEE Transactions On Biometric Image Processing*, Vol. 14, Issue(12), December, 2005.
- [16] Provos, N. and Honeyman, "Hide and Seek: An Introduction Steganography. *IEEE Magazine on Security & Privacy*, pp. 32-44, 2003.