INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 5, Issue 1 SEP 2015

OPTIMIZED BIOMETRIC WATERMARKING APPROACH BASED ON SVD AND DWT

KOKKIRAPATI SAI PRASANNA (PG Scholar) [1]

Mr. *T SRI RAMA MURTHY M.tech Assistant Professor* [2]

Department of ECE, Sri Venkateswara Institute of Science and Information Technology

Abstract

Although tremendous progress has been made in the past years on watermarking for protecting information from incidental or accidental hacking, there still exists a number of problems. A novel watermarking scheme namely iris biometric watermarking scheme is implemented based on SVD and DWT respectively. Digital watermarking is one such technique, where digital embedding of the copyright information/watermark into the data to be protected. The two major ways of doing so are spatial domain and the robust transform domain. In this study, method for watermarking of digital images, with biometric data is presented. The usage of biometric instead of the traditional watermark increases the security of the image data. The biometric used here is iris. After the retinal scan, it is the most unique biometric. In terms of user friendliness in extracting the biometric, it comes after fingerprint and facial scan. The iris biometric template is generated from subject's eye images. The discrete cosine values of templates are extracted through discrete cosine transform and converted to binary code. This binary code is embedded in the singular values of the host image's coefficients generated through wavelet transform. The original image is thus firstly applied with the discrete wavelet transform followed up by the singular value decomposition of the subband coefficients. The algorithm has been tested with popular attacks for analysis of false recognition and rejection of subjects.

KEYWORDS: Watermarking, SVD, DWT, biometric

I. INTRODUCTION

Compared to the old days, it has become super easy to make your information accessible to anyone around the world. That also means that it's trivial for someone to take your information, use it, and claim that it is his own.

As an example, you may take a digital picture of a historical event that you may consider selling to Seattle Times. However, since you're greedy, a human being, and want to maximize the profit, you might've sent the photos to bunch of different companies to make them go on a bidding war. One individual that works at some

company may then modify the image a little bit, claim that it's their original work, and essentially steal it. So what are you left with? Nothing, unfortunately, because you didn't know that you can protect your image even if it's in a digital format. How? You can embed extra information into digitized data to use as a protection—that is what digital watermarking is essentially.

The World Wide Web or WWW phenomena since the late part of the 20th century have demonstrated the commercial potential of free multimedia resources through the digital networks. Multi National Companies (MNCs), for their commercial interests, needs to use the digital networks to offer digital media. However, they also have a necessity of protecting their ownership rights. So here along with cryptography and other alternatives, digital watermarking too, steps in as one of the popular way to accomplish the same. Owing to the advanced copying/replicating tools available to duplicate and modify those multimedia data, security is a major concern. Thus protecting digital multimedia data is very important. There are many types of digital information and data like digital images, audio and video. Watermarking can be either visible or invisible. Visible watermark is used in images and videos but they tend to spoil the beauty and moreover the position of the watermark is disclosed to the attackers in this case.

This led to the popularity of the invisible watermarking, where the position of the watermark is not open to the public. Invisible watermarking may be done either in the spatial domain or the transform domain. The method presented here is of the transform domain variant because of the extra robustness of the same. There are various techniques of implementing transform domain watermarking like Fourier transform, discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD) and many more. Here DWT- and SVD-based hybrid transform domain has been used. This is because the multiresolution property of DWT increases the imperceptibility, whereas SVD aids in improving the robustness of the scheme.

Unlike the traditional methods of using an image or a random signal as a watermark, here the authentication information used as watermark is the iris biometric data of the user. It is used as the user id in this case, similar to various methods that use a logo as watermark. A

biometric is based on the concept of 'something – you-are ', so it increases the security criteria many folds in comparison to the traditional watermarking methods. Biometrics like iris, retinal scan, fingerprint scan, hand geometry, facial scan and so on carries the unique biological information about the user.

Retinal scan is the most secure of these but it is not very user friendly, whereas facial scan, finger print and hand geometry are the most user-friendly but not as much secure as iris or retinal scan. Iris biometric gives an optimized option of user-friendly as well as secure biometric. This is because an iris image of a person can be collected from a distance of couple of meters unlike retinal scan, finger print or hand geometry. Moreover unlike fingerprint once a person is dead his pupils stop dilating so the iris scan of a dead person does not match with a live one. Whereas in comparison to facial scan iris biometrics of twins are not same, and neither do they change with age like the human face.

II. IRIS BIOMETRIC RECOGNITION

Daugman was one of the pioneers in the field of iris-based biometrics and holds patents in this field as well. Wildes et al., Boles and Boashash, Lim et al., Noh et al., Monro and Zhang and Rakshit and Monro followed up the trend with their respective good work. A lot of standard databases have been generated by various institutes to work in this field. Starting from Chinese Academy of Sciences – Institute of Automation (CASIA), Lion's Eye Institute (LEI), Universities of Bath, Carnegie Mellon University, and many more including institutes, even our very own Indian Institute of Technology, Delhi, in India. Here the database used is of University of Bath. The idea here is about identifying the host image and authenticating it through the biometric to avoid colluders. So a very simple methodology has been used to normalise the biometric data in a robust, useable format so that the complexity of the biometrics along with watermarking technology is reduced.

III. WATERMARKING AND IRIS BIOMETRIC TECHNOLOGY

The idea of implementing both the technologies, that is, biometrics and watermarking has been done in two ways. The first, watermarking a biometric data, which is used as a host with a watermark, for protection of the integrity of the biometric data to enhance the security. Whereas the second is where the watermark is a biometric and is used for the

authentication of the host image. Here the work is of the second type. Previously, researchers have used mainly fingerprint and face for this second type of watermarking a host image with a biometric for its protection.

The method used is very simple taken from our previous work. However, out of the various multi-metric techniques proposed, the easiest and the one having lowest complexity, as well as time constraint with significant identification is proposed. The method can be implemented either row-wise or column-wise, in one-dimensional (1D) DCT of the intensities. This is done to obtain the DC coefficients after DCT to give a 1D sequence of DC values for the 2D greyscale iris biometric intensity image. This 1D biometric data here is used as the watermark. The scheme employed here is similar on the lines of hybrid transform.

The DCT of a row of the iris matrix is defined as

$$\mathbf{X_i^n(k,l)} = \mathbf{w(k)} \sum_{\mathbf{l=1}}^{\mathbf{M}} \mathbf{x(n,l)} \cos \frac{\mathbf{(2l-1)(k-1)}}{\mathbf{2M}} \qquad (1)$$

Where , k= 1,2, ……, M

Where x(n,l) is lth sample of the signal in the nth row of the ith iris image, M is the column size, and $w(k) = \sqrt{1/M}$ for k=1 and $w(k) = \sqrt{2/M}$ for $2 \leq k \leq M$

The steps employed, as in Fig. 1, to obtain the iris biometric in 1D watermark format is as under:

The database of eye images obtained from university of bath is taken. There are 20 images of each eye (both left and right) of 20 different persons. Thus we have a database of 2 × 20 × 20 images of which only the left eye images are taken, that is, 400 images. These 400 images are undergone with the normalization and extraction of the iris in a minimum bounded isothetic rectangle (MBIR) format. The MBIR-ed images are processed to obtain rectangular iris templates, normalized to a size of 120 × 200 pixels each. The normalized 120 × 200 iris images are applied with column-wise, 1D DCT and retaining of DC value of each column, to obtain a 1 × 200 set of pixels. These 200 DC values are converted to binary, that is, 200 × 8 bit format and added with CRC-based error control coding.

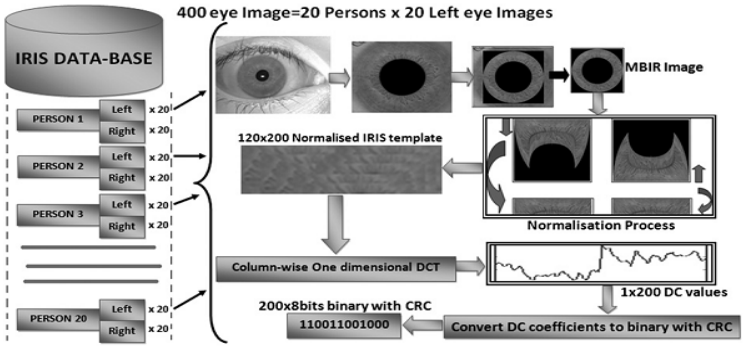

Fig. 1 Iris biometric technology implemented

IV. WATERMARKING METHODOLOGY

The watermarking methodology of using hybrid format of the two robust techniques, that is discrete wavelet transform (DWT) and singular value decomposition (SVD) has been employed here. The host image is applied with the single level DWT using Daubechies (N = 6) wavelet to obtain the four set of coefficients CA, CH, CV and CD. This is followed up by SVD operation on each of them on similar lines, to obtain the two orthogonal matrices U and V and the set of eigen values in S. For the band being CX (here as the same operation is repeated for the approximate band, that is, CA, horizontal band, that is, CH, vertical band, that is, CV and diagonal band, that is, CD the iterative method is referred as CX, that is, CA/CH/CV/CD) the operation is as in the following equation

$$CX = U \times S \times V^{T}, CX = CA/CH/CV/CD \quad (2)$$

The iris biometric watermark is embedded in the eigen value matrix S to obtain S* with CRC200 being the CRC-based 200 DC values of the iris template in binary, as in (3). The CRC used is MATLABs inbuilt CRC-16 cyclic redundancy check codeS. This CRC200 is divided by the threshold KEY; this is to reduce the payload of the embedded watermark (Fig. 2). Then SVD is again applied on the S* matrix to obtain S_1, U_1 and V_1. Here too S_1 is the Eigen value matrix of S*, whereas U_1 and V_1 are the orthogonal matrices. The CRC200 data are added to the modified Eigen value matrix in a linearised way

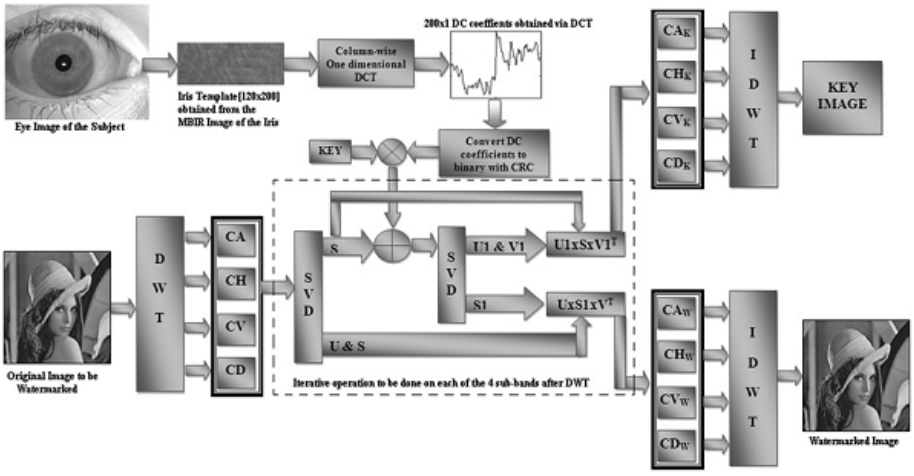

Fig. 2 Iris biometric based image watermarking algorithm

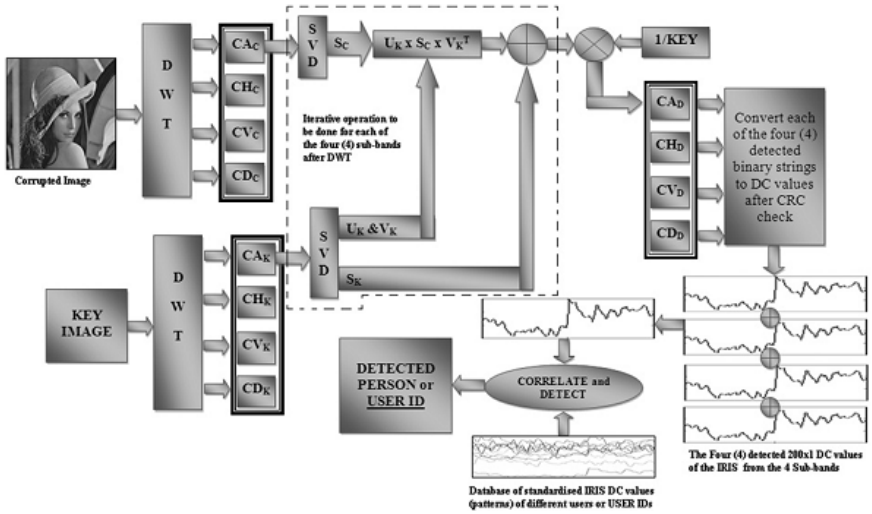

Fig. 3 Watermark extraction and biometric identification algorithm

$$S* = S_1 + CRC_{200}/KEY$$
$$= U_1 \times S \times V_1^T \qquad (3)$$

Now the orthogonal matrices of first SVD operation, that is. U and V are combined with the Eigen values of the second SVD operation, that is S_1 to obtained the subband for watermarked image, that is CW. The rest, that is U_1 and V_1 are combined with the Eigen values of the first SVD operation, S to obtain CK, the subband for the key image. Though they could be

kept as key matrices instead it is preferred to keep them as 'key image' as this would require less memory in place of keeping them as key matrices. In case there are no memory constraints they can be kept as key matrices and be used whereas extraction of the watermark (Fig. 3). Here the word 'key image' refers to the image required during the extraction procedure along with the corrupted image

$$U \times S_1 \times V^T = CW, CW$$
$$= CA_W/CH_W/CV_W/CD_W \quad (4)$$
$$U_1 \times S \times V_1^T = CK, CK$$
$$= CA_K/CH_K/CV_K/CD_K \quad (5)$$

These operations applied on all the four subbands, generate the four subbands for both key image and watermarked image. Then on application of the inverse discrete wavelet transform (IDWT) on the CA_K, CH_K, CV_K, CD_K generates the key image. Similarly, the watermarked image is generated on application of IDWT on CA_W, CH_W CV_W, CD_W.

For the extraction of the watermark from the stego image, the reverse of the above scheme is employed. Here the corrupted version of the watermarked image is considered to be received. Similar to the embedding process, the DWT of the image is taken to obtain the corrupted image's subbands CA_C, CH_C CV_C, CD_C. The image is decomposed back to its respective coefficients as well. Then on each respective subband pair of corrupted image and key image, the SVD is applied to obtain U_C, S_C, V_C, U_K, S_K, and V_K, respectively. The Eigen values of the stego image, S_C are combined with the respective orthogonal matrices U_K and V_K of the key image to generate the stego subband matrix D as in (6). The Eigen values of the key image S_K are then subtracted from the matrix D to obtain the watermark coefficients CX_D for that particular subband after normalisation with the threshold named KEY, as in (7).

This KEY was the multiplying factor applied to CRC DC coefficients to reduce the intensity in the embedding process.

$$D = U_K \times S_C \times V_K^T \quad (6)$$
$$CX_D = (1/KEY) \times (D - S_K) \quad (7)$$
$$CX_D = CA_D/CH_D/CV_D/CD_D$$

So from the obtained watermark coefficients CA_D, CH_D, CV_D, CD_D the four sets of DC values of the iris biometric is obtained. This is done by firstly removing the CRC error control coding redundant bits,

followed by conversion of the binary data to pixel intensities of the DC values. From the set of the four set of DC values detected from the four wavelet subbands a normalised set of DC coefficient is obtained. This obtained set of DC coefficient is correlated with the standard sets of DC coefficient stored for each person for detection, authentication and identification of the biometric watermark. Based on this biometric watermark the person identification or detection of the user id of the subscriber is obtained. This is done using the self-similarity patterns as per our previous work. There it was found that the DC coefficients follow a particular self-similarity pattern for every particular eye. Even the left and right eye of any particular person follows a different set of pattern.

V. RESULTS

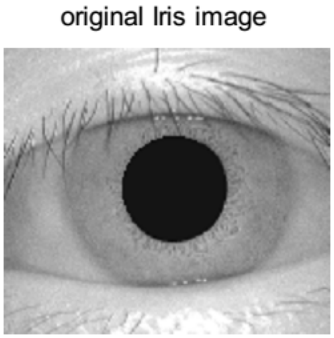

Fig. 4 Original iris image

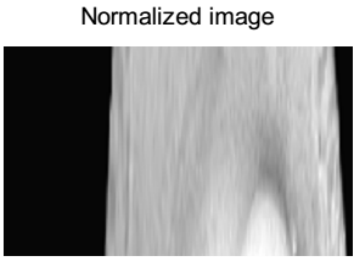

Fig. 5 Normalized image

Fig. 6 Host image

Fig. 7 Watermarked image

VI. CONCLUSION

Here in this paper a non-blind approach of integrating the highly secure iris biometric has been integrated with the image

watermarking algorithm to enhance multimedia security of data. The algorithm here for the biometric generation has been kept very simple to reduce complexity of implementation. Moreover the integration of the SVD and DWT together makes the watermarking scheme robust and imperceptible. Thus this scheme provides a securerobust-imperceptible watermarking technology in total.

REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[2] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding. Steganographyand Watermarking—Attacks and Countermeasures. Boston, MA: Kluwer, 2001.

[3] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Jun. 1997.

[4] M. S. Kankanhalli, Rajmohan, and K. R. Ramakrishnan, "Adaptive visible watermarking of images," in Proc. IEEE Int. Conf. Multimedia Computing and Systems, 1999, vol. 1, pp. 568–573.

[5] Y. Hu and S.Kwong,"Wavelet domain adaptive visiblewatermarking," Electron. Lett., vol. 37, no. 20, pp. 1219–1220, Sep. 2001. [6] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images," in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2000, vol. 2, pp. 1029–1032.

[7] G. Braudaway, K. A. Magerlein, and F. Mintzer, "Protecting publicly available images with a visible image watermark," in Proc. SPIE Int. Conf. Electronic Imaging, Feb. 1996, vol. 2659, pp. 126–133.

[8] Y. J. Cheng and W. H. Tsai, "A new method for copyright and integrity protection for bitmap images by removable visible watermarks and irremovable invisible watermarks," presented at the Int. Computer Symp.—Workshop on Cryptology and Information Security, Hualien,Taiwan, R.O.C., Dec. 2002.

[9] P. M. Huang and W. H. Tsai, "Copyright protection and authentication of grayscale images by removable visible watermarking and invisible signal embedding techniques: A new approach," presented at the Conf. Computer Vision, Graphics and Image Processing, Kinmen, Taiwan, R.O.C., Aug. 2003.

[10] Y. Hu, S. Kwong, and J. Huang, "An algorithm for removable visible watermarking," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 1, pp. 129–133, Jan. 2006.

[11] Y. Hu and B. Jeon, "Reversible visible watermarking and lossless recoveryof original images," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 11, pp. 1423–1429, Nov. 2006.

[12] B. Macq, "Lossless multiresolution transform for image authenticating watermarking," presented at the European Signal Processing Conf., Tampere, Finland, Sep. 2000.

[13] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—Newparadigm in digital watermarking," J. Appl. Signal Process., vol. 2002, no. 2, pp. 185–196, Feb. 002.