Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES)
ISSN: 2566-932X, Vol. 1, Issue 11, February 2018
Proceedings of National Conference on Emerging Trends in VLSI, Embedded and Networking (NC-EVEN 17), May 2017

Iris Biometric Watermarking Using Hybrid Transforms

Aksharasree Anupoju[1], Anupama R[1], Shruthi B M[2]

1. Department Of ECE, REVA ITM, Bangalore, India
2. Department Of ECE, Brindavan College of Engineering, Bangalore, India

Abstract: With the growing popularity of internet, it has become very simple for intruders to amend and generate illegal multimedia data contents. Various techniques of copyright protection of free data are evolved every day. Digital image watermarking is one such technique, where a watermark is digital embedded into the data to be protected. Here, biometric used is iris of a human eye and it is normalised and pre-processed with Discrete Cosine Transform (DCT) to obtain discrete values. An image to be protected is considered and Discrete Wavelet transforms (DWT) and Singular Value Decomposition (SVD) are used to implement the invisible watermarking along with a biometric. The usage of biometric instead of the traditional watermark increases the security of the image data. After the retinal scan, iris is the most unique biometric.

Keywords: Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Iris biometric, Watermarking

I. INTRODUCTION

Enormous growth of the internet in the recent times has made the hackers a traditional business to carry over online. The compatibility for the businessmen and other customers to buy or sell commodities through internet which is possible from any part of the world has become very easily accessible and an essential part of life these days. However, the risk involved in buying or selling things online is directly proportional to the usage of these methods. There can be numerous types of risks on information security, such as theft, corruption or forgery. It has become a very huge issue to secure the rightful ownership. Protecting digital data is always, essential and a must.

A digital data can be moreover a digital image, digital video or digital audio signal. Intruders can duplicate, alter and spread the digital commodities without the notice of the owners. Encryption methods play a very vital role in shielding the digital data. The different methods of encryption are cryptography, stenography, digital watermarking, etc. Digital watermarking is one of the best and the safest methods of encryptions.

Watermarking is a process of embedding copyright information or a watermark into the data that is publicly displayed. Digital watermarking refers to the watermarking on the digital data such as digital image or audio or video. There are different types of watermarking, namely, visible watermarking and invisible watermarking. Visible watermarking can be embedded into an image or video but they tend to spoil the original beauty of the digital data. In this case, the position of the watermark is disclosed which can make it easy for the hackers. This disadvantage of the visible watermarking led to the development of the invisible watermarking. In invisible watermarking, the position of the watermark is secured. It can be carried over in spectral domain, spatial domain or hybrid domain. The spatial domain deals with modification of the bits or with the bit-planes. A bit-plane is a plane which is created by one specific bit of every pixel. The spectral domain deals with transforms such as Discrete Cosine Transform (DCT) and Fast Fourier Transforms (FFT). The hybrid domain deals with Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD).The combination of SVD and DWT based hybrid-domain watermarking is being used in this project. It is because of the multi-resolution property of the DWT that increases the imperceptibility and robustness property of the SVD. Using a logo, a text or an image as a watermark is the conventional way to protect the digital data that is easily available, to hack the copyright information. The use of biometric data as an authentication, aids in the utmost safety of the copyright information. Biometrics like finger-print, hand-geometry, facial-scan, retinal-scan, iris, etc., carries unique biological information about the user. Every individual has their own distinctive features of the biometric data. In this project, the iris biometric data of an individual is used. Iris is considered as the wholly secured biometric because of its characteristics. No iris of an eye will be similar to the iris of another eye. The iris of a person's left eye is also not similar to his/her right eye. The pupil dilates after the death of a person which further leads to the change of the iris and leading into mismatch with the iris of the live ones.

A. Digital Watermarking Life- Cycle Process:

The signal where the watermark will be embedded is called the host signal. The system is separated into 3 different steps, embedding, attack and detection. In the embedding process, an algorithm is generated to embed watermark on to the host signal to generate a watermarked signal. The watermarked signal is then transmitted over a channel. If any person tries to alter the watermarked signal, it is called an attack. The process of attack generally refers to the attempt made by an intruder

NC-EVEN was held at Brindavan College of Engineering, Bengaluru, India on 11th May, 2017.

to eliminate the watermark through any means of modification of the signal that is being transmitted. Detection is an algorithm that is being applied to the attacked signal. It is done to extract the original watermark from the image. If the signal was not altered, then the watermark can be extracted without any complexity or without any loss of data.

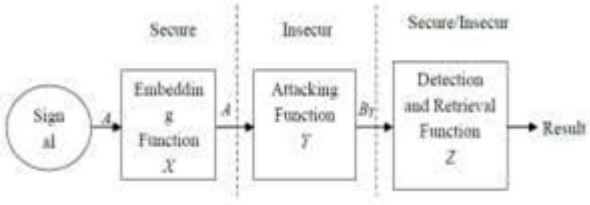

Fig 1. Generalised life-cycle of digital watermarking.

B. *Techniques Of Digital Watermarking:*

The techniques used in digital watermarking can be given in the form of a block diagram as,

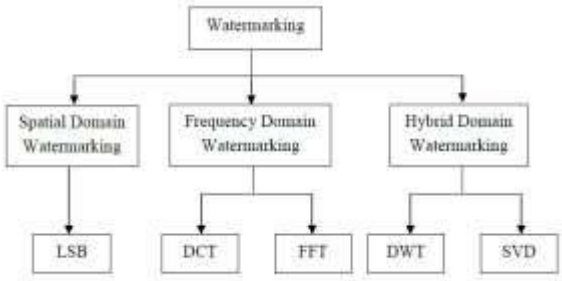

Fig 2. Techniques of digital watermarking.

C. *Biometrics*

Unlike the conventional methods of using an image or any random signal as a watermark, we make use of the iris biometric data of the user as the authentic information as watermark. Biometrics is the modern trend of information protection technology. Compared with existing traditional security systems, biometric systems are much more user friendlier and difficult to scam because the biometric traits are unique for every person and are stable throughout his/her life, i.e., it is based on the perception of 'something that you are'.

Iris biometric gives an optimised form of user-friendly as well as well secured biometric. The reason is, an iris image of a person can be collected from a distance of couple of meters differently when compared to retinal scan, finger print or hand geometry. Moreover, when a person is dead his fingerprints can be easily taken away which is dissimilar in the case of iris image which dilates when the person is dead. It will get collapsed and after sometime of death, his pupils start dilating. Thus the iris scan of a dead person does not match with a live one. Also, the iris biometric in comparison to facial scan, they are not same for twins, and neither do they transform with age like the human face.

II. METHODOLOGY

The idea to implement biometrics and watermarking technologies is carried over by a using biometric as the watermark which is used on the host image and will be more authenticated when compared to the method of watermarking a biometric, which is used as a host with a watermark. The usage of fingerprints or the face as biometrics has become very ordinary and the safety has reduced which increases the risk.

The method used is less complex, chosen out of the various multi-metric techniques proposed, the simplest method having less time constraint as well with proposed significant identification. The method can be either implemented by a row-wise or column-wise one dimensional (1D) Discrete Cosine Transform (DCT) of the image. The formula for 1-D DCT is given below.

$$F(u) = \lambda(u)\sum_{i=0}^{N-1} f(i)\cos\left\lfloor \frac{\lceil \pi.u \rceil}{\lfloor 2.N \rfloor}(2i+1)\right\rfloor \quad (1)$$

A. *Iris Methodology:*

In this project, we consider the iris as the biometric. An eye of a person is taken and we crop the image to extract the iris features. We consider the Minimum Bounded Isothetic Rectangle (MBIR) format in which only the iris features are extracted and the other feature i.e., the pupil of an eye is rejected. Then the extracted image is further normalised to the required size. In this project, we make use of a column-wise DCT which results in a row of values. This is performed on the normalised eye image to obtain the DC values for the iris biometric image. These DC values are given as an input to the in-built CRC (Cyclic Redundancy Check) generator which generates a 16-bit binary sequence.

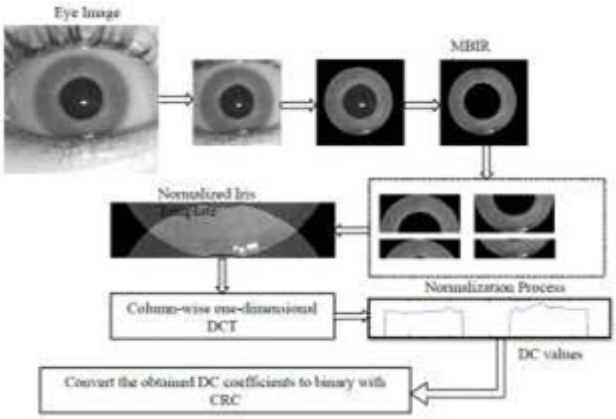

Fig 3. Process of extraction of iris from an eye

B. Watermarking Methodology:

An image is considered, which is to be authenticated and Discrete Wavelet Transform (DWT) is applied on the image. On application of DWT on an image, an image get divided into four sub-bands namely, Approximate Sub-band (CA), Horizontal Sub-band (CH), Vertical Sub-band (CV), Diagonal Sub-band (CD). Each of the obtained four sub-bands is carried over with an interaction function part. The interaction function part through which the sub-bands go through is comprised of the combination of Singular Value Decompositions (SVDs).

CA Approximate sub-band	CH Horizontal sub-band
CV Vertical sub-band	CD Diagonal sub-band

Table 1. 1-D Discrete Wavelet Transform decomposition.

A SVD can be applied only on data having 2 component values such as a grey scale image. Since we consider an image which has 3components, as DWT applied to this image will also result in the same, i.e., the sub-bands obtained will also comprise of the same components. The three components, namely, the Red, Green and Blue components are commonly known as the RGB components of the image. Therefore, SVD is applied to all of these components individually and then combined together to form the U, S & V components of the SVD output.

$$\sum_{i=0}^{r} \quad ,(2)$$

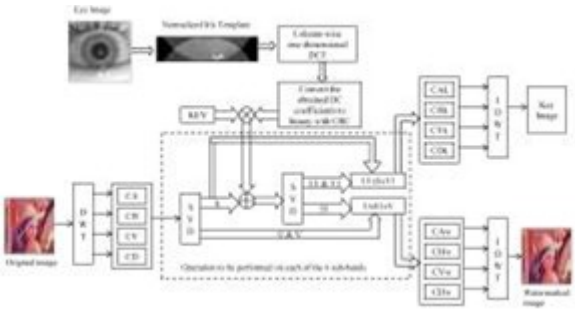

Fig 4. Iris biometric image watermarking methodology

In this project, the watermarking methodology makes use of the two hybrid techniques namely DWT and SVD. The host image is transformed with single level DWT with Daubechies wavelet where N=6, to obtain the four sub-bands. These sub-bands are CA, CH, CV and CD. These sub-bands are then processed with a combination of SVDs on each of them. The combination of SVDs can be shown in the above figure. On application of the first SVD, we obtain two orthogonal matrices U and V and a set if eigenvalues in the form of a diagonal matrix also known as the singular matrix S.

The iris biometric watermark is embedded in the singular matrix S to obtain S*. The obtained CRC is added with a key. The SVD is again applied on the matrix S* to obtain S1, U1 and V1. The obtained S1 is the singular matrix of S* and U1 & V1 are the orthogonal matrices.

The orthogonal matrices of the first SVD i.e., U and V are combined with singular matrix of the second SVD i.e., S1 to obtain the sub-band for the key image i.e., CK. And the rest of the matrices, U1, S and V1 are combined together to form the sub-band for the watermarked image i.e., CW. This key image is used in the de-watermarking part or during the extraction part along with the watermarked image.

These operations are applied on all the four sub-bands, to generate the four sub-bands for both the watermarked image and the key image. Then we apply the inverse discrete wavelet transform (IDWT) on to generate the key image. Similarly, we apply IDWT on to generate the watermarked image.

III. RESULTS

In this project, we consider an eye image of a person as shown in the figure 5 to extract iris from it to use it as a watermark.

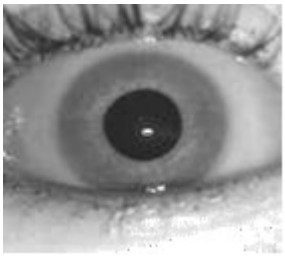

Fig 5. Eye Image of a Person

The following pictures as shown in figure 6 shows the extraction of iris and then cropping into halves and combining them to extract the iris data.

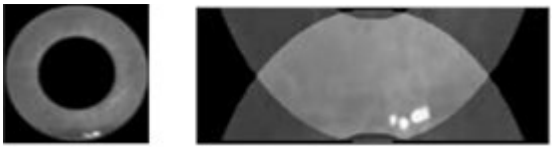

Fig 6. Extraction of iris from the eye image

The 1-D DCT is applied on the obtained iris data to obtain the DC values as plotted in the figure 7

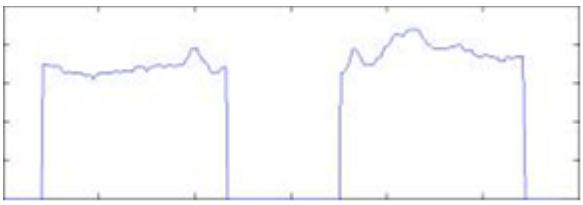

Fig 7. DC Values of the considered eye image

Next, we consider image as shown in figure 8 as the original image which is to be watermarked.

Fig 8. Original Image

On applying 1D- DWT to the original image, with Daubechies wavelet where N=6, we obtain the output as shown in the following figure 9.

Fig 9. 1-D DWT on the Original image which results in four sub-brands

After the process of watermarking on the iris image and the original image to be watermarked, we obtain a watermarked image, as shown in figure 10.

After the processing, we obtain four different sequences of binary data for each of the four sub-bands . They are shown in figure 11.

Fig 10. Watermarked Image

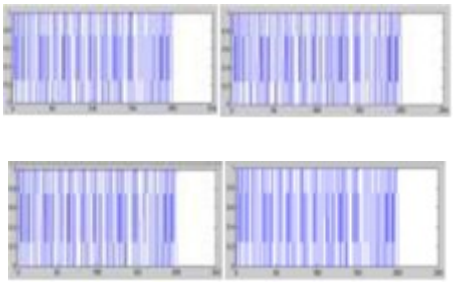

Fig 11. Plots of the binary sequences of the output sub-bands.

MSE	76.05dB
PSNR	29.12dB

Table 2. MSE AND PNR VALUES

The MSE and PSNR values are 76.05dB and 29.12dB respectively.

IV. DISCUSSION

The method of watermarking with iris biometric highly secures the digital data and combining SVD & DWT together makes the watermarking scheme more robust and imperceptible. The algorithm proposed is to be implemented based on the objective of authenticating the data based on a person's own genuine identity i.e., iris. Thus it helps in partially reducing the attacks on the data to be secured.

REFERENCES

[1] "Robust SVD-based Audio Watermarking Scheme with Differential Evolution Optimization", Baiying Lei, Ing Yann Soon, IEEE Transaction on Audio, Speech, And Language Processing Aug 21, 2013.

[2] "A Robust QR- Code Video Watermarking Scheme Based On SVD and DWT CompositeDomain",G.Prabakaran, R.Bhavani, M.Ramesh, IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013".

[3] "Singular value decomposition and wavelet based iris biometric watermarking", Swanirbhar Majumder, Kharibam Jilenkumari Devi, Subir Kumar Sarkar, IET Biom., 2013, Vol. 2, Iss. 1, pp. 21–27 & The Institution of Engineering and Technology 2013 doi: 10.1049/iet-bmt.2012.0052

[4] "A Digital Watermarking Algorithm based on DCT & DWT", Mei Jiansheng, Li Sukang1 and Tan Xiaomei, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107

[5] "Invisible Digital Watermarking In The Spatial and Dct Domains For Color Images", Heather Wood, Adams State College, Alamosa, Colorado "An introduction to biometric recognition,"

[6] K. Jain, A. Ross, and S. Prabhakar, IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.

[7] "Novel Iris Biometric Watermarking Based on Singular Value Decomposition and Discrete Cosine Transform", Jinyu Lu, Tao Qu, and Hamid Reza Karimi, Hindawi Publishing Corporation, Mathematical Problems in Engineering, Volume 2014, Article ID 926170