IRIS BIOMETRIC WATERMARKING USING SINGULAR VALUE DECOMPOSITION AND WAVELET BASED TRANSFORM

ANOOPA C J
F. Student/ME CSE, Coimbatore institute of technology Computer science and engineering, Coimbatore, India.

Abstract – Recent technological advancements have made it very easy for intruders to modify the multimedia contents transmitted over the network. Digital watermarking is a such technique, where digital embedding of the copyright data or watermark into the data to be protected. The two major ways of doing that protection are spatial domain and the robust transform domain. The spatial domain method is comparatively simple. Since it lacks the basic robustness that may be expected in any watermarking applications, it is not much used nowadays. The product of high quality watermarked image is by first transforming the original image into the frequency domain by the use of Fourier, Discrete Cosine Transform (DCT) or Discrete Wavelet transforms (DWT) and Singular Value Decomposition (SVD) . In this paper, biometric data is used for watermarking of digital images. The usage of biometric data substituted in the place of the traditional watermark leads to the increase in the security of the host image. The biometric that is being used here is human iris. The discrete cosine values of iris templates are extracted through Discrete Cosine Transform (DCT) and converted to binary code. This binary code is then embedded into the singular values of the host image’s coefficients generated through discrete wavelet transform. The result of this project is that the person’s identity is detected using his iris image. Compared with the previous existing works DWT-DCT, support vector regression (SVR)-DWT-DCT, DWT-SVD method obtains more robustness against the selected attacks.

Keywords- SVD, DWT, DCT, Iris Embedding, Image Watermarking, Biometric Watermarking.

I. INTRODUCTION

Since the late part of the 20th century, the world wide web has demonstrated the commercial potential of free multimedia resources through the digital networks. However, the multinational companies which are using these multimedia resources also have a necessity of protecting their ownership rights. So here comes with cryptography and other techniques like digital watermarking to accomplish the same. Thus protecting digital multimedia data is very important. It is also becoming easier for some individual or group to copy and transmit digital products without the permission of the owner. The digital watermark is then introduced to solve this problem. Covering many subjects such as signal processing, communication theory and Encryption, the research in digital watermark is to provide copyright protection to digital products, and to prevent and track illegal copying and transmission of them. Watermarking is embedding information, which is able to show the ownership or track copyright intrusion, into the digital image, video or audio. Its purpose determines that the watermark should be indivisible and robust to common processing and attack.

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 it provides extra robustness. There are different techniques of implementing transform domain watermarking like Fourier transform, discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD) etc. Here DWT- and SVD-based hybrid transform domain has been used. This is because the multi resolution property of DWT increases the imperceptibility, whereas SVD helps in improving the robustness of the system. 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.

Biometrics is the current trend of information security technology. It determines the identity of a person based on his/her biophysical features (e.g. face, fingerprint, palm-print, and iris), or behavior features (e.g. signature, voice, and gaits). Various biometric systems have been developed during the past decades and some of them such as automated fingerprint recognition systems (AFRS), iris recognition systems, and face recognition systems have been successfully applied in a wide range of applications, including access control, attendance control, and customs checking, etc. Compared with existing traditional token based security systems, biometric systems are much user friendlier and difficult to fraud because the biometric traits are unique to every person and are permanent throughout his/her life, ie it is based on the concept of ‘something that you are’. Iris biometric gives an optimised form of user-friendly as well as
secure biometric. The reason is that, 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, even when a person is dead his fingerprints can be easily taken which is different in the case of iris image which stops dilating when the person is dead and will get collapsed after sometime of death his pupils stop dilating. Thus the iris scan of a dead person does not match with a live one. Another point in favour of iris biometric is that, in comparison to facial scan iris biometrics of twins are not same, and neither do they change with age like the human face.

II. RELATED WORK IN LITERATURE

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. A related work has already been done as in face feature watermarking. A paper on DWT-based multiple watermarking says that embedding a visual watermark in both low and high frequencies will result in a robust scheme that can resist to different kinds of attacks. Embedding at low frequencies increases and widens the robustness when referred to attacks that posses low pass characteristics like filtering, lossy compression and geometric distortions while turning the scheme more sensitive to modifications of the image like histogram, and contrast/brightness adjustment and many more. The biometric forms like iris, retina, fingerprint, face and so on carry unique identity of a person. Thus they are used for the secure authenticity of any person. Retina is the most secure of all the biometric methods even if it is not user friendly. Face and finger are highly user friendly but not as secure as iris or retina.

III. PROPOSED SYSTEM IMPORTANCE OF SINGULAR VALUE DECOMPOSITION

SVD is defined with respect to a theorem from linear algebra, which specifies that a rectangular matrix \( A \) of size \( m \times n \) can be split into the product of three matrices \( U \) and \( V \) and the transpose of orthogonal matrix \( V \) of size \( n \times n \). It is been defined as follows,

\[
\text{SVD}(A_{m\times n}) = U_{m\times m}S_{m\times n}V_{n\times n}
\]

By multiplying \( U \) and the matrix \( A \) is obtained.

\[
A_{m\times n} = U_{m\times m}S_{m\times n}[V_{n\times n}]^T
\]

the matrix \( S \) are the left singular vectors, i.e., the columns of \( U \), and are the right singular vectors, i.e., the rows of \( (\text{or columns of } V) \). \( U \) and \( V \) are unary matrices that means , where and are the unit matrices. The eigen-vectors of \( AA^T \) make up the columns of \( U \) and the Eigen-vectors of \( A^TA \) are the columns of \( V \). The diagonal element of \( S \) represents the square root of the Eigen values of either \( AA^T \) or \( A^TA \).

In signal processing applications, SVD technique has been applied to processes like image compression, noise reduction and image watermarking. SVD transforms provide an elegant method for extracting algebraic features from an image. Using SVD in digital image processing has different advantages. The major advantage is that, singular values in a digital image are highly stable, that is, when a small perturbation is added to image, it’s singular values do not change significantly. Another fact is that, singular values contain intrinsic algebraic image properties. It is significant to note that each singular value specifies the luminance of image while the corresponding pair of left and right singular vectors specify the geometry of the image layer. If the magnitude of the singular values is increased, that will increase the image luminance, which lowers the magnitude and thus decreasing the image luminance. It means that singular values are in close relation with the image luminance, while the intrinsic “geometry” of the image depends upon left and right singular vectors which are orthogonal matrices. These all characteristics of SVD make it very much desirable for watermarking.

IV. IMPORTANCE OF DISCRETE WAVELET TRANSFORM

In mathematics, a wavelet series is the best representation of a square integrable (real or complex valued) function by certain orthonormal series generated by a wavelet. This article provides a formal, mathematical definition of an orthonormal wavelet and of the integral wavelet transform. The wavelet transform can provide us with the frequency of the signals and the time associated to those frequencies, making it very convenient for its application in various fields. For example, signal processing of accelerations for gait analysis. In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time). The discrete wavelet transform has a huge number of applications in science, engineering, and mathematics and computer science. Most importantly, it is used for signal coding, to represent a discrete signal in a more redundant form, often is a preconditioning for data compression.
The idea of implementing biometrics and watermarking together can be 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. And the second is where the watermark is a biometric and is used for the authentication of the host image. Here the proposed 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.

And the second is where the watermark is a biometric and is used for the authentication of the host image. Here the proposed 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 DCT is done to obtain the DC coefficients 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 Discrete Cosine Transform (DCT) of a row of an iris matrix is defined as follows with \( k = 1, 2, \ldots, N \) where \( x(n, l) \) is the \( l \)-th sample of the signal in the \( n \)-th row of the \( i \)-th iris image, \( M \) is the column size, and \( w(k) = \sqrt{1/N} \) for \( k = 1 \) and \( w(k) = \frac{\sqrt{2/N}}{2} \) for \( 2 \leq k \leq N \).

\[
X^n_l = w(k) \sum_{n=1}^{N} x(n,l) \cos \left( \frac{2\pi(n-1)(k-1)}{2N} \right) \quad (3)
\]

The eye images are processed to obtain rectangular iris templates normalised to a size of 120 × 200 pixels each. The normalised 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.

The watermarking methodology of using hybrid format of the two robust techniques, that is discrete wavelet transform (DWT) and singular value decomposition (SVD) is being explained as follows. The host image is applied with the single level DWT using Daubechies wavelet to obtain the four set of coefficients CA, CH, CV and CD. This is followed 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 (the same operation is repeated for the approximate band CA, horizontal band CH, vertical band CV and diagonal band CD, the iterative method is referred as CX, CA/CH/CV/CD) the operation is like given in the following equation

\[
CX = UX \times S \times V^T \quad (4)
\]

where, \( CX = CA/CH/CV/CD \).

The eigen value matrix \( S \) is embedded with the iris biometric watermark to get \( S^* \) with CRC 200 being the CRC-based 200 DC values of the iris template in binary.

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 CRC 200 data are added to the modified Eigen value matrix in a linearised way.

\[
S^* = S^*_1 + CRC_{200} \quad (5)
\]

Now the orthogonal matrices of first performed SVD operation, ie \( U_1 \) and \( V_1 \) are combined with the Eigen values of the secondly performed SVD operation ie \( S^*_1 \) to obtain the subband for watermarked image ie \( CW \). The remaining, those is and are combined with the Eigen values of the first SVD operation, \( S \) to obtain \( CK \), the subband for the key image. They could have been kept as key matrices but instead of that it is more preferred to keep them as ‘key image’ as this would require less memory in place of keeping them as key matrices. Here the word ‘key image’ refers to the image required during the extraction procedure along with the received (corrupted) image.

\[
U \times S \times V^T = CW, \quad (5)
\]

\[
CW = CA_{W}/CH_{W}/CV_{W}/CD_{W} \quad (6)
\]

These operations are applied on only one subband CH, which generate the four subbands for both key image and watermarked image. Then on application of the inverse discrete wavelet transform (IDWT) on the \( CA_K, CH_K, CV_K \) and \( CD_K \) generates the key image as mentioned earlier. Similarly, the watermarked image is generated on application of IDWT on \( CA_W, CH_W, CV_W \) and \( CD_W \). The exact reverse of the above scheme is employed, for the extraction of the watermark from the stego image. Here a corrupted version of the watermarked image is considered to be received. Just like the embedding process, the DWT of the corrupted image is received, is taken to obtain the corrupted image’s subbands \( CA_K, CH_K, CV_K \), and \( CD_K \). The image is decomposed back to its respective coefficients. Then on CH subband pair of corrupted image and key image, the SVD is applied to obtain \( UC_K, SC_K, VC_K, UC_W, SC_W, \) and \( VC_W \) respectively. The Eigen values of the stego image, SC are combined with the respective orthogonal matrices \( UC_K \) and \( VC_K \) of the key image to generate the stego subband matrix D. The matrix D is the one which is converted to DC values and then the CRC is applied.
IRIS Biometric Watermarking Using Singular Value Decomposition And Wavelet Based Transform

V. EXPERIMENTAL ANALYSIS

The integration of the SVD and DWT together makes the watermarking scheme robust and imperceptible. All the coefficients of the DWT can be embedded with the watermark. The algorithm is observed to be attack resistant to copy attack and noise. The proposed work has proved to be more efficient from the existing ones that are on fingerprint and face biometric watermarking. The results are based on the number of detections of the original persons identity using the embedded watermark.

The PSNR values of both face and iris embedded images differ (Figure 1.4). The PSNR value of face embedded watermarking is around 44dB but for iris biometric watermarking using SVD and DWT is above 50dB (see Table 1.0).

CONCLUSION

The paper proposes a method of watermarking done with iris biometric and the key concepts like SVD and DWT. The algorithm proposed in this paper is developed solely based on the objective of authenticating a person based on his own genuine identity that is iris. The result is a robust method of authentication which can survive attacks and produce the output of the persons authenticity.

<table>
<thead>
<tr>
<th>Type of watermarking</th>
<th>face</th>
<th>iris</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCT watermarking</td>
<td>37</td>
<td>40</td>
</tr>
<tr>
<td>DWT watermarking</td>
<td>39</td>
<td>41</td>
</tr>
<tr>
<td>SVD and DWT</td>
<td>44</td>
<td>50</td>
</tr>
</tbody>
</table>

Table 1.0: PSNR values of watermarking schemes

REFERENCES

IRIS Biometric Watermarking Using Singular Value Decomposition And Wavelet Based Transform


★★★★