IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

Hybrid DWT and SVD based biometric watermarking for fingerprint authentication

Komal Ramteke[1], Swati Ramteke[2]

Assistant Professor, Department of Information Technology, Rajiv Gandhi College of Engineering and Research, Nagpur, India[1]

Scholar, SKN Sinhgad Institute of Technology & Science. Lonavala, Pune, India[2]

Abstract*:* Biometric predicated authentication system has inherently advantage over traditional personal identification techniques. A critical problem is to ascertain the security and integrity of biometric data. Digital watermarking is a technique that is utilized to solve this problem. This paper represents a hybrid DWT and SVD based biometric watermarking algorithm which is utilizable for embedding watermark i.e. binary equivalent of minutiae of fingerprint into cover fingerprint image. Here we select lower resolution band for embedding watermark as watermark detection is computationally efficient at lower resolution band. The proposed algorithm can satisfy the transparency and robustness of the watermarking system very well and even in the presence of different image processing attacks utilizable information can be extracted accurately from fingerprint images.

Keywords: Digital watermarking, DWT, SVD, Arnold transform, Copyright protection.

I.INTRODUCTION

With the development of network and multimedia technologies, multimedia copyright security and content authentication have become severe problem that need to be solved. Multimedia and network security issues are classically handled through cryptography; however, cryptography ascertains confidentiality, authenticity, and integrity only when a message is transmitted through a public channel such as an open network. It does not protect against unauthorized replicating after the message has been successfully transmitted. Digital watermarking is an effective way to secure copyright of multimedia data even after its transmission. Among the different biometrics, fingerprints are more famous in the authentication area, as they are unique to each person and are widely utilized in identification and verification of personal individuality. However, they are vulnerable to accidental and intentional attacks, when transmitted over network. Thus, a defensive scheme is needed which will preserve fidelity and prevent modifications. Digital watermarking technology provides dynamic solution for it. Digital Image Watermarking is a technique which provides solution for copyright, image authentication and other issues. Watermarking deals with decomposing original image called cover image utilizing some wavelet transforms and embedding watermark into one of the sub band (LL,LH,HL,HH) the obtained image is called watermarked image, this image have transmitted through channel where different noise affect watermarked image. At receivers side embedded watermark has extracted from watermarked image.

There are many methods to embed the watermark. It can be divided into two classes: spatial-domain watermarks and transform-domain watermarks. The spatial domain is so simple that the watermark can be damaged facilely, but the transform-domain algorithm can be resist intensity attack, watermark information can't be damaged easily. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT). The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients.

In this paper, we introduce hybrid DWT and SVD predicated watermarking method for fingerprint images and this method can be utilized in steganography-based application to embed minutiae data in fingerprint images. The utilization of a biometric data (fingerprint image) to cover another one (fingerprint minutiae) increases the ability of security because the unauthorized person who obtains the fingerprint image watermarked is liable to treat the fingerprint image instead the hidden minutiae data. The objective of this watermarking scheme is to ascertain secure transmission of minutiae details even over a noisy communication channel or over one subject to intentional tampering.

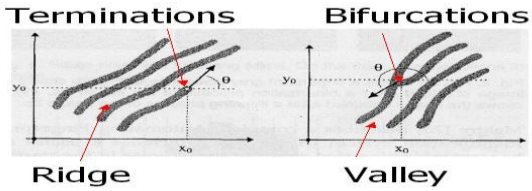
II. FINGERPRINT MINUTIAE

A fingerprint is made up from an impression of the pattern of ridges on a finger. Each person has his own fingerprint with the permanent uniqueness. So fingerprint has being utilized for identification and forensic investigation for a long time. A fingerprint is composed of many ridges and furrows. However, shown by intensive research on fingerprint apperception, fingerprints are not distinguished by their ridges and furrows, but by Minutiae, which are some eccentric

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

points on the ridges (Fig.1 (a)). Minutiae points are most generally the locations of ending or bifurcation of ridges in an exceedingly fingerprint.

(a)



(b)

Fig.1. (a) A typical fingerprint image showing
(b) Minutiae. (Valley is also referred as Furrow, Termination is also called Ending and Bifurcation is also called Branch)

III. WATERMARK EMBEDDING PRINCIPLES

A. Discrete Wavelet transforms (DWT)

Wavelet transform is a time-frequency domain cumulated analysis method. It has multi-resolution analysis features. Each level of the wavelet decomposition has four sub-images with same size. Let the LLk stands for the approximation sub image and LHk, HLk, and HHk stand for the horizontal, vertical and diagonal direction high-frequency detail sub image respectively. Where the variable k = 1,2,3,...(k ∈ N) is the scale or the caliber of the wavelet decomposition. DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The rudimentary conception of discrete wavelet transform in image process is to multi-differentiated decomposing the image into sub image of different spatial domain and independent frequencies.

After wavelet decomposition, many signal processing, such as compression and filter are liable to transform the high frequency wavelet coefficients. If the watermark sequence is embedded into this component, its information may be disoriented in the processing in sequence, which will reduce the robustness of the watermark. In order to ascertain the watermark has a better imperceptibility and robustness, the approximation sub-image LL3 coefficients are opted to embed watermark. We can achieve the transform of the separable wavelet as in Fig.2.

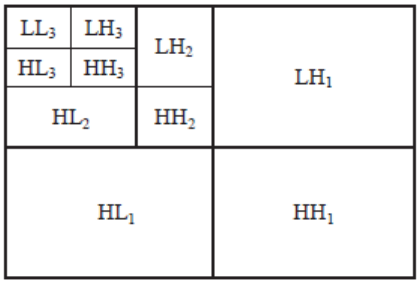


Fig.2. Three level wavelet decomposition

B. Singular Value Decomposition (SVD)

If a m*n image is represented as a real matrix A, it can be decomposed as:

$$A = U S V^T$$

It is called a singular value decomposition of A . Where U is a m*m unitary matrix, S is a m*n matrix with nonnegative numbers on the diagonal and zeros on the off diagonal, and V^T denotes the conjugate transpose of V, an n*n unitary matrix. The nonnegative components of S represent the luminance value of the image. Transmuting them scarcely does not affect the image quality and they also don't change much after attacks, watermarking algorithms make use of these two properties.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

C. Arnold Transform

Arnold transform is commonly called as elegant face transform, it randomizes the original organization of pixels in a real image. However, if iterated enough times, the pristine image reappears. Arnold transform is the position shift of one to-one point. Arnold transformation on digital image of size N×N defined by Eq. 1 is a one-to-one transformation.

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \pmod N \quad (1)$$

Where i, j ∈ {0, 1, ...,N-1}.

Where (i, j) is the location coordinates of the real image pixels and (i', j') is the location coordinates of image pixels that after transform When all the coordinates are transformed, the image we get is scrambled images.

IV. PROPOSED WATERMARKING ALGORITHM

In the proposed approach, initially the watermark image is produced by extracting the minutiae points (ending, bifurcation) from fingerprint image and then converted to binary watermark image. Next the cover fingerprint image is decomposes into 3-level two-dimensional DWT coefficients and the approximation sub-band LL3 is opted to embed watermark .The produced watermark image is additionally undergo Arnold transformation before embedding process is perform. After that by applying SVD concept on watermark image and selected sub-band of cover image, the watermarked image coefficients are produced. Then inverse DWT is apply to determinately generate the watermarked image in which the watermark is embedded. The watermark extraction process is performing in precisely the inversion order of watermark embedding process.

The proposed watermarking scheme for fingerprint images has been shown in fig. The cover image is the fingerprint while the watermark is a binary image identically equal to the minutiae of the cover fingerprint. The scheme has been divided into two sections:

A. Watermark Embedding
B. Watermark Extraction.

A. Watermark Embedding scheme:

The steps of embedding watermarks can be described as follows.

Step1: The fingerprint image is decomposed into its 3-level two-dimensional DWT coefficients. Out of the all sub-bands, only LL_3 approximation sub-band is preferred. (Denotes as A).

Step 2: Fingerprint Pre-processing

An authentic fingerprint might have discontinuities that might lead to spurious minutiae. Consequently, minutiae extraction is preceded by fingerprint pre-processing, which involves normalization, ridge orientation and frequency estimation. Determinately, the ridge orientation and frequency estimation values are utilized for filtering the fingerprint using Gabor wavelet. Gabor filtering enhances the ridges oriented in the direction of the local orientation, and decreases anything oriented differently. Hence, the filter increases the contrast between the foreground ridges and the background, at the same time, efficiently reducing noise. The filtered output is then binarized and thinned to one-pixel width.

Step 3: Minutiae Extraction

Minutiae points such as end points and bifurcation points are recognized by calculating Crossing number (CN). CN value is defined as half the sum of the distinguished between pairs of adjacent pixels in the eight neighbourhoods.

$$CN=0.5 \sum_{i=1}^{8} |P_i - P_{i+1}|, \quad P_{1=} P_9$$

where Pi is the pixel value in the neighbourhood of a pixel P.

If crossing Number is 1, 2 and 3 or larger than 3 then minutiae points are classified as Termination, Normal ridge and Bifurcation respectively. The only minutiae of interest are ridge endings and bifurcation (corresponding to *CN*=1 and *CN*=3 respectively).From the extracted minutiae points x and y co-ordinate, ɵ (orientation of ridges) and type of minutiae i.e. termination or bifurcation are obtained. Type of minutiae can already be set as 0 for ending and 1 for bifurcation, making it a binary format . The remaining three columns of minutiae can be converted into binary form representation and a binary watermark is generated by concatenating the eight individual bit planes and binary watermark (W) from minutiae is produced.

Step 4: Perform Arnold transform for watermark image W.

Step 5: We obtain the watermarked image coefficients matrix A_W through the following three steps:

1. $A = USV^T$
2. $S + \alpha W = U_W S_W V_W^T$ where α is watermark strength
3. $A_W = US_W V^T$

Step 6: Apply inverse wavelet transform for original image, and then altering the double-precision real number to unsigned 8-bit integer. Thus, obtain the watermarked image in which watermark are embedded.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

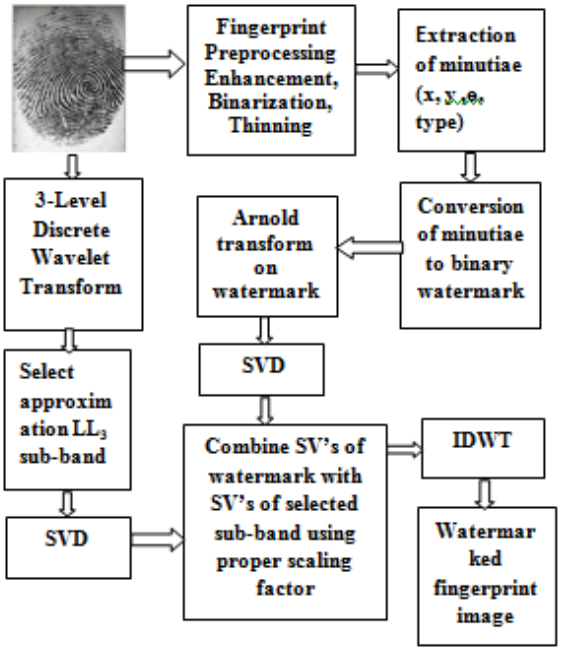


Fig.3. Diagram of embedding watermark

B. Watermark (Minutiae) Extraction scheme:

We can extract the watermark by the inverse calculation of watermark embedding:

Step 1: Perform a 3-level wavelet transform using haar wavelet for watermarked image, and obtain low-frequency wavelet coefficient LL_3 (denotes as A*).

Step 2: Apply SVD to the A*, such that $A^* = U^* * S_1^* * V^{T*}$, and obtain U^*, S_1^* and V^{T*}.

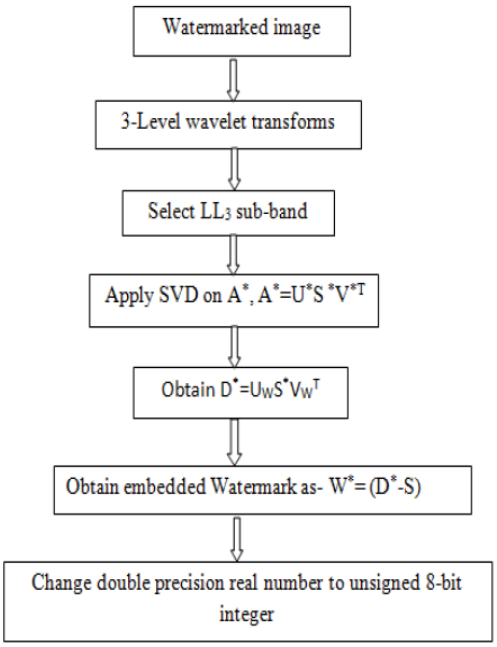


Fig.4. Diagram of extracting watermark

Step 3: Now by using values of U w, V_W and S_1 *, obtain D* according $D^* = U_W S_1 * V^T$, in the end we can obtain the watermark which is embedded according to $W^* = (D^* - S) / \alpha$.

Step 4: Conclusively transmuting the double-precision real number to unsigned 8-bit integer for watermark image, and perform inverse Arnold transform for watermark image.

Step 5: Minutiae points are then regenerated by stacking bit planes and converting them back to decimal system.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

We specified the verification precision of extracted watermark when watermarked fingerprint is attacked by different image processing attacks. The verification precision is calculated in terms of normalized coefficient which is considered as relatives attribute measure between embedded watermark and extracted watermark without any attack and under attacks. The NC under no attack is 0.9888 which proves that the minutiae information i.e. binary watermark is accurately extracted without degrading the visual quality of host fingerprint image.

V.CONCLUSION

In this paper, we proposed watermarking scheme is based on hybrid transform domain DWT and spatial domain SVD for fingerprint images. Due to spatio-frequency resolution of DWT, it offers more degrees of liberation as compared with DCT. The main objective of this scheme is to provide security and robustness to fingerprint images. The watermark (i.e. binary identical of minutiae) is embedded into LL_3 sub-band because watermark detection at lower resolution is computationally efficient. Additionally in order to ascertain watermark has better imperceptibility and robustness, the approximation sub-image LL_3 coefficient is opted to embeds watermark. Applying Arnold transform to watermark image makes result even better Subsequently the embedded watermark can be extracted from watermarked image effectively under normal extraction or even in the presence of different image processing attacks.

REFERNCES

[1] D. Mathivadhani, C. Meena, “A Comparative Study on Fingerprint Protection Using Watermarking Techniques”. In Global Journal of Computer Science and Technology, vol. 9, no. 5, pp. 98-102, 2010

[2] Weimin Yang, Xiaoning Zhao,” A Digital Watermarking Algorithm Using singular Value Decomposition in Wavelet Domain” 978-1-61284-774-0/11,2011 IEEE.

[3] Ms.Jalpa M.Pate1, Mr.Prayag Patel, “A brief survey on digital image watermarking techniques”. In International Journal for Technological Research in Engineering Volume 1, Issue 7, March-2014 ISSN.

[4]Ravi. J, K. B. Raja, Venugopal. K. R,”Fingerprint recognization using minutiae score matching”. In International Journal of Engineering Science and Technology Vol.1 (2), 2009, 35-42.

[5] Sachin Mehta, Rajarathnam Nallusamy, Ranjeet Vinayak Marawar, Balakrishnan Prabhakaran, “A study of DWT and SVD based Watermarking Algorithms for Patient Privacy in Medical Images”. In 2013 IEEE International Conference on Healthcare Informatics.

[6] Khalil Zebbiche, Lahouari Ghouti, “Protecting Fingerprint Data using Watermarking”. In Proceedings of the First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06) 0-7695-2614-4/06, 2006 IEEE.

[7] Rajlaxmi Chouhan, Pritee Khanna, “Robust Minutiae Watermarking in Wavelet Domain for Fingerprint Security”. In World Academy of Science, Engineering and Technology 60 2011.

[8] R. Chouhan, A. Mishra, P. Khanna, “Wavelet-based robust digital watermarking scheme for fingerprint authentication”. In Proc. International Conference on Intelligent Computational Systems, pp. 29-33, 2011.