IJARESM
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING, SCIENCE & MANAGEMENT

A REVIEW ON WATERMARKING TECHNIQUES FOR BIOMETRIC SECURITY

Rimmi K Patel
PG Student, Electronics and Comm. Dept., SCET, Surat, Gujarat, India

Abstract: ***In this era of modern technology, it has become easy for adversaries to bypass the conventional identity authentication and identification processes, hence modern security systems have been developed to a great extent to provide protection of privacy and security of identities in different applications. An application where biometric data are used as identification and authentication of individual, security of biometric data is essential. Robust Watermarking provides a means to hide crucial data called watermark, into cover signal such that it is kept secret and can be utilized later to prove the ownership of cover signal. To increase the security level and verification accuracy of biometric based personal identification system, one biometric data is hidden into another biometric data. As transform domain techniques are robust, they have gained popularity over spatial domain techniques. It is not always possible to have original signal for extraction, blind watermarking techniques are preferable.***

1. INTRODUCTION

In recent years, the utilization and deployment of biometric authentication system is becoming increasingly popular in commercial, educational, industrial, and government sectors. As compared to traditional authentication techniques such as token based or knowledge based techniques where, PIN codes, IDs and passwords need to be remembered, biometric based systems are gaining popularity. The reason behind this popularity is the ability of biometric data to easily and efficiently discriminate between an authorized person and an imposter, who acquire access privilege of an authorized person. General Biometric Authentication System is shown in Figure 1.

Biometric data of a person is sensed using sensor and features are extracted using feature extraction algorithm at feature extractor. This extracted feature, also called biometric template is stored in database during enrolment phase. During verification phase, the candidate template is compared with the stored templates in database at matching module. Matching module generates matching score. Based on matching score, decision is made whether the candidate is authorized person or an imposter.

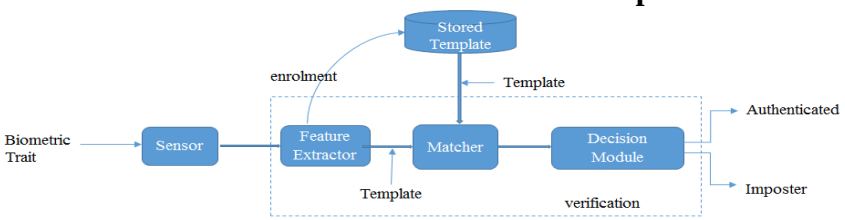

Figure 1 Biometric Authentication System [1]

Biometric data is not secret because person leaves his/her fingerprint on every surface he touches. It is not replicable as well. Due to these reasons, various attacks are possible in this type of authentication system as shown in Figure 2.

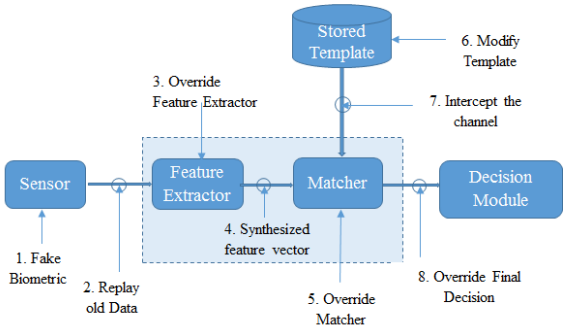

Figure 2 Biometric Authentication System with possible attacks [2]

1. Fake biometric is presented at the sensor
2. Previously intercepts biometric data is resubmitted to the system
3. Feature extractor is forced to generate feature value chosen by the attacker instead of actual value generated from data obtained from sensor.
4. Feature extracted from the data obtained from the sensor is replaced with the synthetic feature set.
5. Matcher is forced to produce high/low matching score regardless of input feature set generated from data obtained from sensor.
6. The attack on template stored in database for example, adding a new template, modifying an existing template, removing template etc.
7. The channel between matcher and database is compromised which is resulting into the alteration of transmitted template.
8. Final attack includes altering of matching result itself.

To prevent biometric data from these attacks, the approaches such as Encryption, Staganography and Watermarking are used. Encryption is not preferred for providing security to biometric data because, once the encrypted data is decrypted, the media is no longer protected. Staganography and watermarking both are data hiding methods but objective and condition for both the techniques are different. Staganography is basically used for secret communication while Watermarking is used for content authentication and ownership protection.

Classification of Watermarking Techniques

Watermarking techniques are classified according to types of documents, domain of watermark embedding, watermark extraction, ability of watermark to resist attacks and visibility. It can be seen in Figure 3 in detail.

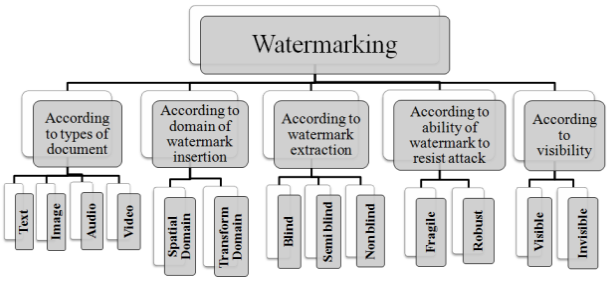

Figure 3 Classification of Watermarking Techniques

Requirements of Watermarking Technique

Watermarking security means that without damaging the host signal, the watermark should be difficult to remove or alter. Capacity, Robustness and Imperceptibility, these three are mutually conflicting requirements of information hiding scheme. The security requirement of watermarking system can differ slightly depending on the application. These requirements cannot be optimized simultaneously. There is always a trade-off between these three requirements. Capacity refers to the amount of information that can be embedded into host signal. Imperceptibility refers to the perceptual transparency of the watermark. Ideally, no perceptible difference between the original signals should exist. Robustness refers to the capability of the watermark to survive signal manipulations.

2. WATERMARKING APPROACHES

Various intentional as well as an accidental attacks are possible in biometric based authentication system. Among these attacks, communication channel attack is more serious. Consider Biometric Authentication System shown in Figure 1.2. For verification purpose, template stored in database is transmitted through channel, which is received by matching module and compared with the candidate template. Sensor, feature extractor, matching module and decision module is assumed to be at receiver side and database is assumed to be at transmitter side. Transmitter and receiver sides are assumed to be under supervision. Communication channel between transmitter and receiver is not secure because an attacker can easily access the data. To prevent the biometric data to be altered by attacker, it is hidden into a cover image. This data hiding is achieved by watermarking technique

Spatial Domain Watermarking Techniques

The amplitude modulation based watermarking method was proposed in [1], where fingerprint image was used as cover image and face information i.e. Eigen-face coefficients were used as watermark. In Embedding process, face features are extracted and converted into binary bit stream. To find the location for embedding the watermark, a random number generator is used which is initialized with a secret key. The watermarked image is then generated by modifying host image pixels. In most of the watermark applications, to recover the embedded data without knowing the host data is desired, therefore a simple and effective blind watermarking algorithm is proposed [2]. Based on the characteristics of an image, one area and its nearby region are correlated. If the pixels are nearer, the correlation among those pixels is high. Here, different area having sizes of 3 x 3, 5 x5, 7 x 7 and 9 x9 which is also called a mask is selected to approximation the value of luminance of its central pixel in the area. This is shown in figure. 2.1. The value of luminance of the central pixel is highlighted by O in the Figure. 4.

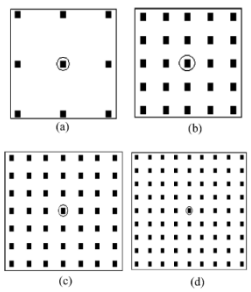

Figure 4 Estimation of the central pixel with the nearby pixels in an area in different sizes (a) 3x3 (b) 5x5 (c) 7x7 and (d) 9x9.[4]

The mean value of luminance of all the nearby pixels of the central pixel is computed in selected area of particular mask size. Embed watermark bit one by one with the following rule: To embed watermark bit '1', real value of luminance is made higher than mean value of luminance by changing the luminance of the central pixel. And to embed watermark bit '0', real value of luminance is made lower than mean value of luminance by changing the luminance of the central pixel.

Transform Domain Watermarking Techniques

1. Discrete Fourier Transform based Watermarking technique proposed in [5][6] uses the concept of Local Feature Region (LFR). Edges and corners resides in an image are considered as features of an image. This feature is taken as a centre and circular region is selected. This circular region around the feature is called Local Feature Region (LFR). These LFRs obtained from host image carry the watermark. Hence they can be viewed as independent channels. Similar copies of watermark are inserted into all channels to improve the robustness of transmitted information. The block diagram of embedding scheme is shown in Figure. 5

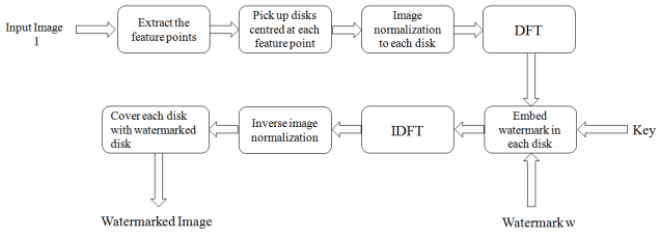

Figure 5 Block diagram of watermark embedding process in DFT domain [5]

Detector consists of all the above process but in inverse manner. One major disadvantage of this technique is that it requires original watermark image for extraction process. And this technique is computationally complex. Hence DFT base techniques are not popular and wavelet domain techniques are preferred over them.

2. Discrete Wavelet Transform based Watermarking Techniques

When the watermark bits are embedded in the significant coefficients of the whole frequency domain, watermarking becomes more robust. Many block-based watermarking methods have been proposed, these methods cannot resist attacks efficiently because a watermark bit is embedded in the block of coefficients of size n x n and the significant coefficients are not considered. Maximum wavelet coefficient quantization method is proposed in [7] to solve the above problems. In this, the variable numbers of wavelet coefficients are grouped into a block from the LH and HL sub bands, and then the maximum coefficient of the block is quantized to embed a watermark bit. Then, researchers introduced Redundant Discrete Wavelet Transform (RDWT). In Redundant Discrete Wavelet Transform based Watermarking Technique proposed in [8], the colour face image is decomposed into red, green and blue channels which will increase the embedding capacity. If watermark bits are inserted into red and blue channels, watermark will becomes imperceptible. But when green channel is used to hide the watermark, the watermark will become visible as noise. In this algorithm, first the appropriate location is calculated for embedding the watermark in the face image, and extracting the watermark for verification.. To achieve high capacity, RDWT based technique is used.

3. Discrete Cosine Transform based Watermarking Techniques

The technique proposed by Choi and Aizawa in [9] estimates the DC component of a central block using four DC components around that central block which can be seen from Figure. 6. If a spatial RGB colour image is considered as a host, it is converted into YUV component where Y component is divided into 8 x 8 blocks and DCT is computed. Each nine 8 x 8 blocks are selected as a group to estimate the DC component of the central block with the help of DC components in its nearby 4 blocks. Once the DC component of central block is estimated, the actual DC value of the central block is replaced with its estimated value by modifying it with +Δ or -Δ according to the embedded watermark bit that is '1' or '0'. The group is having total 9 blocks, but only 4 blocks are used to approximate the DC component in the central block, These 4 blocks are shown as grey in colour in Figure. 6

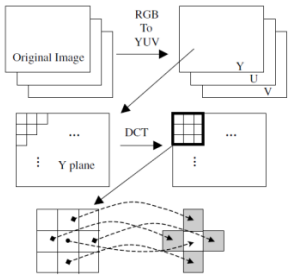

Figure 6 Estimation of the DC component in the central block using four DC components in the up, down, left and right block.[4]

Block 1 DC1	Block 2 DC2	Block 3 DC3
Block 4 DC4	Central Block DC5	Block 6 DC6
Block 7 DC7	Block 8 DC8	Block 9 DC9

Figure 7 The central block (gray colour) and its adjacent blocks.[4]

Estimation of DCT AC coefficients based method proposed in [3] adjusts the DC value adaptively. The energy compaction characteristic of DCT is utilized here to estimate the AC coefficients. Here, only the DC values of a 3 x3 neighbourhood of 8 x 8 blocks are required to estimate the AC coefficients of the central block shown in Figure. 7. The estimation formulae for the first five unquantized DCT AC coefficients are shown in equations given below.

$$AC(0, 1) = 1.13884 \times (DC4 - DC6)/8$$
$$AC(1, 0) = 1.13884 \times (DC2 - DC8)/8$$
$$AC(0, 2) = 0.27881 \times (DC4 + DC6 - 2 \times DC5)/8$$
$$AC(2, 0) = 0.27881 \times (DC2 + DC8 - 2 \times DC5)/8$$
$$AC(1, 1) = 0.16213 \times (DC1 + DC9 - DC3 - DC7)/8$$

In Embedding Process, the first step is to select every nine 8 x 8 blocks as one group. In each group, 5 watermark bits can be embedded by modulating the 5 AC components shown in above equation. Watermark bits can be embedded using the following translation rule: Set $ACi \geq ACi' + \Delta$ to insert bit '1' and Set $ACi \leq ACi' - \Delta$ to insert bit '0'. Where, ACi is real value of one of the 5 AC Components, and ACi' is estimated value of ACi. Δ is reference threshold (5-15 % of the original ACi value). ACi is the real value of one of the 5 AC components: AC(0,1), AC(1,0), AC(0,2), AC(2,0) and AC(1,1). ACi' is the approximated value of ACi using equations given for AC estimation. Δ is a reference threshold and can be

selected as 5–15% of the original ACi value. For extraction the watermark following condition is checked and then decision is taken whether the extracted bit is '1' or '0' If ACi ≥ ACi' retrieved bit is '1' and if ACi ≤ ACi' retrieved bit is '0'. If ACi is equal to ACi', there is uncertainty about whether the watermark bit is a '1' or '0'.

3. CONCLUSION

Few of the watermarking techniques are reviewed and it is concluded that transform domain based technique is preferred to secure biometric data because it can embed more bits of watermark and resist more attacks than spatial domain techniques. Moreover a biometric data is very crucial so that a blind or semi blind watermarking technique is preferred over other non blind techniques. Two techniques can be combined as per requirement of application.

REFERENCES

[01] Anil K. Jain,Umut Uludag, Student Member, IEEE, "Hiding Biometric Data,"IEEE transactions on pattern analysis and machine intelligence, vol. 25, no. 11,pp.1494-1498 November 2003

[02] Anil K. Jain, Karthik Nandakumar "Biometric Authentication: System Security and User Privacy", Magazine, IEEE Computer Society, November 2012.

[03] Juergen Seitz, "Digital Watermarking For Digital Media", Information Science Publishing, 2005

[04] Yulin Wang, Alan Pearmain, "Blind Image Data Hiding Based on Self Reference", Pattern Recognition Letters, pp.1681–1689, Elsevier 2004.

[05] Xiang-yang Wang, Li-min Hou, Jun WuA, "Feature-Based Robust Digital Image Watermarking Against Geometric Attacks", Image and Vision Computing 26, pp. 980–989, Elsevier 2008.

[06] Wei Lu, Hongtao Lu, Fu-Lai Chung, "Feature Based Robust Watermarking Using Image Normalization", Computers and Electrical Engineering journal, pp.2-18 Elsevier 2010.

[07] Wei-Hung Lin, Yuh-Rau Wang, Shi-Jinn Horng, Tzong-Wann Kao, Yi Pan, "A Blind Watermarking Method Using Maximum Wavelet Coefficient Quantization", Expert Systems with Applications journal 36, pp. 11509–11516, Elsevier 2009.

[08] Mayank Vatsa, Richa Singh, Afzel Noore, "Feature Based RDWT Watermarking For Multimodal Biometric System", Image and vision computing journal, pp.293-304, Elsevier 2007.

[09] T.D. Hien, Z. Nakao, Y.-W. Chens, Robust multi-logo watermarking by RDWT and ICA, Signal Processing – Fractional Calculus Applications in Signals and Systems, Vol. 86, pp.2981–2993, January 2006.

[10] Y. Choi and I. Aizawa, "Digital Watermarking using Inter Block Correlation," in Proceedings of the International Conference on Image Processing, vol. 2, pp. 216–220, October 1999.

