Histogram-based Watermarking Technique for Securing Biometric Templates

Shweta Setiya
Research Scholar, Department of Computer Science and Applications, Kurukshetra University, Kurukshetra-136119
Email: shwetasetiya25792@gmail.com
Chander Kant
Assistant Professor, Department of Computer Science and Applications, Kurukshetra University, Kurukshetra-136119
Email: ckverma@rediffmail.com

Abstract

Now-a-days, internet is used everywhere, but sometimes it becomes bane instead of boon. With the rapid growth of internet, its security issues have also been raised side by side. Security in biometric is also required to avoid it from intruders. Securing the templates in the database has gained the attention of researchers. Biometric system is different from other system in its way of using biometric traits instead of PINs and passwords which have chances of being stolen or forgotten. Thus, templates needs to be accessed only through authenticated users, which could be achieved by using techniques like liveness detection, watermarking, steganography etc. Watermarking is a technique of embedding the watermark into the host image to generate authentic image for storing in database instead of original host image.

Keywords: Biometric security, Biometric histogram, Template Protection, Watermarking.

1. Introduction

The word Biometric is combination of two words- Bio meaning Life and Metrics meaning Measurements. Biometric system consists of five modules namely- sensor, feature extractor, database, matcher, and decision module. Biometric system is used for authenticating and authorizing a person on the basis of something that he have i.e. the biometrics traits(fingerprint, face, retina, hand geometry, iris, gait, keystroke, signature) unlike passwords and PINs which have chances of being forgotten, stolen and easily guessed. Every human being is unique in terms of these traits. These traits get stored in the database of biometric system in the form of templates during enrolment process. After enrolment, biometric system enters either in identification or verification mode. The templates stored in the database need security so that any unauthorised user cannot have access to the database. Several techniques are there for securing templates and watermarking is one among them. Digital watermarking is a promising technique to tackle the problem of copyright protection which has become a major issue worldwide [1].

2. Problem Statement

Many types of attacks are possible in the biometric system as shown in Fig 1. A template compromise may involve the replacement or modification of the stored biometric template of an enrolled user to substitute the template of an unauthorised user, or the addition of the template of an unauthorised user. In the former case, the impostor would assume the identity of an authorised user and be able to perform any actions permitted to that user. However the authorised user would thereafter be unable to access the system and this may lead to the discovery of the compromise. Adding a new template would effectively illegally enrol the impostor on the system. Existing users would be unaffected, which may lessen the chance of detection. In order for this form of attack to be successful the integrity of the template database would have to be seriously undermined. Many techniques are there for securing the templates.

Watermarking is one of the technique used for the copyright protection of digital media. In watermarking, proprietary information(such as signature, logo, ID number etc.) is embedded into digital contents(like image, audio and video) without changing its perceptual quality. It modifies the templates by embedding watermark into it so that an attacker cannot have access to the original templates. Once the template will be lost it cannot be replaced as it could be done with passwords. The watermark contains key information about the authenticate user. It is embedded invisibly into the digital image so that also accounts for the characteristics of the HVS(human visual system). If the attacker manages to have access to the database containing watermarked templates then it will be of no use to him.

Characteristics of digital watermarking process are:-

- Robustness: Watermark should be difficult to remove from digital image. It should withstand attacks like compression, filtering, rotation, scaling, cropping, translation etc.
- Imperceptibility: quality of cover image should not get degraded after embedding watermark into it.
- Capacity: amount of data to be embedded in the

digital content and techniques that make embedding possible.

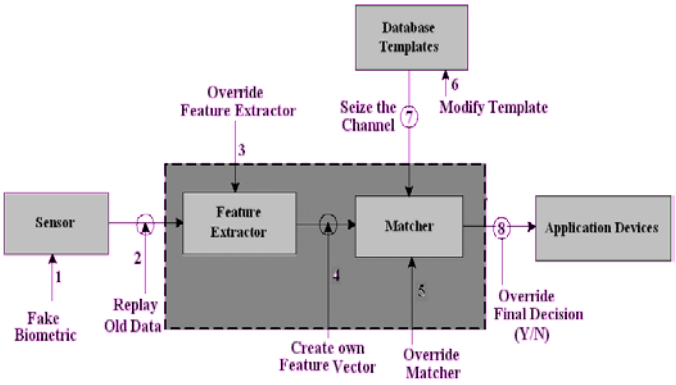

Figure 1: Vulnerabilities in a biometric system [2]

- Blind watermarking: no requirement of original image for the extraction of watermark.
- Security: The embedded information must be secure against tampering.

3. Classification of Watermarking Techniques

Techniques developed so far for the watermarking of images can be categorized as:[3]

3.1 According to watermark insertion scheme

3.1.1. Spatial domain techniques [4][5] directly works on the pixel values by embedding watermark in LSB of some randomly selected pixels e.g.- Least Significant bit (LSB) method.. These methods are easy to implement and incur low cost. But the watermark is not robust i.e. it can be easily destroyed if watermarked image is low-pass filtered or JPEG compressed[5].

3.1.2. The transform domain technique is more robust because in it the image is first transformed using Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT) or combination of both DFT and DCT and then watermark is embed using water embedding method.

3.2 According to human visibility

3.2.1. Visible watermarks, which are embedded in such a way that they are visible when content is viewed.

3.2.2. Invisible watermarks, also called transparent watermarks follow the imperceptibility characteristic of digital watermarking process.

3.3 According to attack resisting ability of watermark

3.3.1. Robust watermark, that should be difficult to remove from digital image and should withstand attacks.

3.3.2. Fragile watermark, that gets destroyed when watermarked data is modified.

3.4. According to key used

3.4.1 Asymmetric, that uses different keys for embedding and detecting watermarks.

3.4.2. Symmetric, that uses same key for both purposes.

3.5 According to watermark detection and extraction

Blind and non-blind watermark. Original image is required for extraction process in non-blind whereas original image is not required for detection and extraction in case of blind watermark technique.

There are two types of attacks:- signal processing attacks(such as compression, filtering, and noise addition) and geometric attacks(such as scaling, rotation, shearing, cropping, and random bending). The watermark technique should be able to resist all these attacks.

4. Related Work

Histogram based method has been used for watermarking. Yong et.al.[6] randomly selected the pixels for transferring from one bin to another which resulted in more change in the pixels values though the method outperforms other methods for common signal processing and geometric attacks.

Agya mishra et.al. [7] have proposed alpha blending technique for watermarking. It uses two scaling factors (k and q) multiplied by low frequency parts of the host and watermark image and added. Experiment has been conducted on a image with 10 different values of k and q, and it has been observed that when k= 0.0009 and q= 0.0022 the results outperforms the other results. Problem with this technique is that original image is to be saved for using it during watermark extraction.

Alpha blending technique has been used by other researchers also for their experiments.[8] They examined the technique on a datasets of size 8 out of which the best result is at k=0.85 and q=0.009.

Watermarking technique has been presented in spatial as well as transform domain. In transform domain, DWT, DCT and combination of both are used[3].

5. Watermark Embedding Process

Fig 2. shows the watermark embedding process of proposed method. It consists of 4 steps- discrete wavelet transform, histogram construction, embedding range selection, watermark embedding.

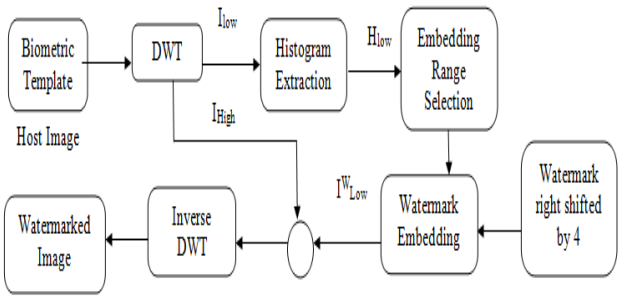

Figure 2: Watermark Embedding Process

5.1 Discrete wavelet transform

Firstly we will consider a host image and apply 3-level DWT(Discrete Wavelet Transform) on it. Discrete wavelet transform is a method used for splitting an image into different frequency bands i.e., low, medium and high thus offering multi-resolution representation of image. The low frequency part is also called approximation because it contains almost all information about the image while the high frequency part has information about edge component only. So if we will embed the watermark in low frequency part it may degrade the image and watermark may become visible destroying the imperceptibility property.

However, embedding in low part is robust. Embedding in high frequency part follows imperceptibility property as edge changes are less sensitive to human eye[8].

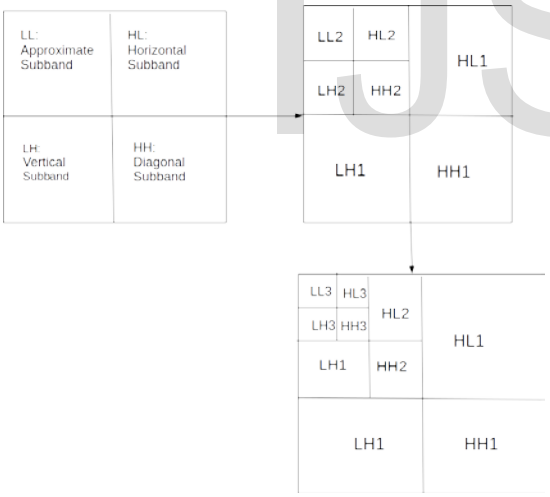

Figure 3: 3-level discrete wavelet decomposition

After first level decomposition, there are 4 sub-bands: LL1,LH1,HL1 and HH1. For each successive level of decomposition, LL sub-band of previous level is considered as the input and divided into 4 sub-bands. Finally after third level of decomposition, there are total of 10 sub-bands.

5.2 Histogram construction

Histogram of an image is a plot that represents the number of pixels versus the gray level values. It provides a convenient summary of intensities in an image, but unable to convey any information regarding spatial relationships between pixels [9]. Histogram based methods have potential to tackle cropping, RBAs(Random Bending Attacks) and other geometric attacks(like rotation, scaling, translation) as histograms are independent of pixel positions. Histogram of an image I with gray levels in range[0, L] can be expressed as:-

$H= \{h (i) | i=0,1,...,L\}$ (1)

where h (i) denotes the number of pixels corresponding to *i*th gray level and

$X*Y = h (i)$ (2)

where X is the total number of rows of I and Y is total number of columns of I. In an 8-bit image, we have 256 gray levels ranging from 0 to 255. I(x, y) denotes the intensity value of a single pixel(within [0, 255] in case of 8-bit image) where (x, y) stands for the position of pixel.

After applying DWT on the host image, its low-frequency component I_{low} is extracted and histogram of this component is constructed i.e $H_{low.}$

5.3 Embedding Range Selection

In this step, the location where we have to embed the watermark is extracted. After constructing the histogram of low-frequency component $H_{low,}$ we combine the neighbouring three(L_B) gray levels to form a bin. Then numbers of bins are denoted as-

$B_n = floor(L / 3)$ (3)

Number of pixels in a group are denoted by $h_{B(i)}$. The bin vector B is expressed as

$B=\{ b (i) | i=0,1,....,floor(255/3)\}$ (4)

The combining process can be formulated as

$b(i) = h_{low}(2*i) + h_{low} (2*i + 1) + h_{low} (2*i + 2)$ (5)

Further we consider two neighbouring bins as a group and define the group vector D as

$D = \{ d(i) | i=0,1,...,floor(255/6)\}$ (6)

Denote the number of pixels in each group by $h_{G(i)}$. Next we have to find out the pixel groups that will be used for embedding the watermark bits. For pixel group selection we will consider g(i) that being the ratio between number of pixels in a group and total number of pixels in the host image i.e

$g(i) = h_{G(i)}/N$ (7)

where N denotes the total number of pixels in the host image selected for embedding the watermark and i=255/4. If the value of g(i) is greater than a predetermined threshold T_G then the *i*th pixel group is selected for watermark embedding else leave that group. The value of T_G is chosen as

$T_G = N/4*L_B$ (8)

here L_B is chosen as 3, therefore T_G=N/12. If the number of pixels in a group become large, then the value of g(i) will also increase correspondingly which means higher robustness but the lower embedding rate as few pixel groups will be chosen for watermark embedding. Let us consider that N_G pixel groups are suitable for watermark embedding

$N_G <= floor(M_B/2)$ (9)

The number of watermarks to be embedded are denoted by N_W. If $N_G = N_W$, all of the N_G pixel groups are chosen for embedding. If $N_G < N_W$ then those pixel groups with higher g(i) values are selected. In order to make sure that these selected groups should be properly identified during decoding phase even after some

attacks, a safe band is introduced in the form of a gap between N_w chosen groups and non-chosen groups in the embedding process. Non-watermarked groups are scanned to check the number of pixels, N_d. If N_d is greater than predetermined threshold T_a, then $N_d - T_a$ pixels are randomly selected and moved from non-watermarked group to the nearest watermarked group such that they are no longer in the gray levels related to the non-watermarked group but belongs to the gray levels in the nearest watermarked group. The value of T_a is based on X and Y i.e. $T_a = 0.004*X*Y$. It controls robustness and visual quality.

5.4 Watermark Embedding

In each selected group we have two bins b1 and b2. Let us denote the number of pixels in the bins by N_{b1} and N_{b2} and watermark is right shifted by 4 in order to decrease its value and distortion in the host image. The watermark sequence is denoted by

$$W = \{w(i) \mid i=0,1,....,L\}$$

Following embedding rule for *k*th watermark bit is used:-

$$N_{b1}/N_{b2} >= 2, \quad \text{if } w(k) = 1$$
$$N_{b2} / N_{b1} >= 2, \quad \text{if } w(k) = 0 \qquad (10)$$

When w(k) is 1 and N_{b1}/N_{b2} is not greater than 2, then a certain number of pixels say N_1 are transferred from b1 to b2 such that N_{b1}/N_{b2} >=2. Similarly if w(k)=0 and N_{b2} / N_{b1} is not greater than 2, then some pixels say N_0 are transferred from b2 to b1. N_1 and N_0 can be calculated as

$$N_0 = 2N_{b1}-N_{b2}/3$$
$$N_1 = 2N_{b2}-N_{b1}/3 \qquad (11)$$

Transferring pixels from one bin to other will have impact on the visual quality of the image. In order to reduce the degradation of the image, the amount of pixel value changes during the pixel transfer should be small. If we assume to embed the watermark bit o into some 'x' group and N_{b2} / N_{b1} is not greater than 2 then in [6][10] we have to randomly select N_0 pixels to transfer from b2 to b1. This situation will lead all randomly selected pixels to jump at least L_B gray levels contributing to negative impact on perceptual quality.

Here, we propose a new pixel transfer method to reduce the pixel movements.

If w(k) is 1 and N_{b1}/N_{b2} is not greater than 2, then to transfer N_1 pixels from bin_2 to bin_1 follow-

- If $N_{ki.LB+1} >= N_1$, then choose all N_1 pixels from grey level $K_{i.LB+1}$.
- If $N_{ki.LB+1} < N_1$, then choose $N_{ki.LB+1}$ pixels from grey level $K_{i.LB+1}$ and the remaining $N_1 - N_{ki.LB+1}$ pixels from other grey levels in bin_2.

The pixels selected in bin_2 are moved to grey level $K_{i.LB}$ in bin_1.

If w(k) is 0 and N_{b2}/N_{b1} is not greater than 2, then to transfer N_0 pixels from bin_1 to bin_2 follow-

- If $N_{ki.LB} >= N_0$, then choose all N_0 pixels from grey level $K_{i.LB}$.
- If $N_{ki.LB} < N_0$, then choose $N_{ki.LB}$ pixels from grey level $K_{i.LB}$ and the remaining $N_0 - N_{ki.LB}$ pixels from other grey levels in bin_1.

The pixels selected in bin_1 are moved to grey level $K_{i.LB+1}$ in bin_2.

After embedding all watermark bits into the image, we have the low-frequency component of watermarked image(I^W_{low}). Combine this component with high-frequency component(I_{high}) of host image I to form watermarked image.

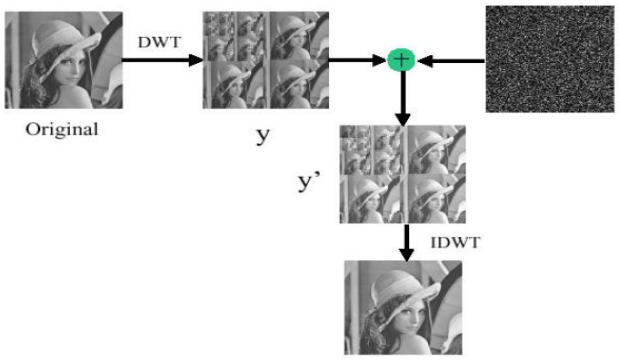

Figure 4: Proposed Model for watermarking

6. Watermark Extraction Process

Fig. 5 shows the process of watermark extraction. Here we are not required to save the host image for extracting watermark which becomes the advantage of this work. We only need the received image thus the security is increased.

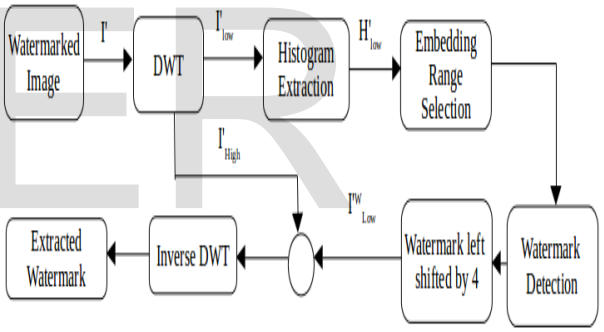

Figure 5: Watermark Extraction Process

Step 1: We have watermarked image I' with X rows and Y columns in data matrix form.

Step 2: DWT is applied on I' to obtain its low-frequency component.

Step 3: Construct histogram H'_{low} from I'_{low} follow the same steps as in section-3. Divide the histogram into bins and groups, each group having two bins bin_1 and bin_2.

Step 4: Compute number of pixels in bin and group and then compute N' and g'(i) by referring to (7). Groups with highest g'(i) values are chosen as watermarked groups.

Step 5: In *i*th watermarked group, denote number of pixels in bin_1 and bin_2 by N'_{b1} and N'_{b2} respectively. If N'_{b1}/N'_{b2}>=1, then extracted watermark bit is 1, otherwise it is 0.

The process is repeated until all watermark bits are extracted. After extraction the watermark sequence is left shifted by 4 and is represented by

W'= { w(i) | i=0,1,2.....L}

7. Conclusion

In this paper, an algorithm of watermarking technique for securing the biometric template is proposed. Embedding of watermark is done in the low-frequency component in order to increase the robustness of the image. Discrete Wavelet Transform method has been presented for decomposing the image into different frequency sub-bands to identify the range for embedding the watermark. Histogram is used to cope with geometric attacks. Instead of DWT, DCT or combination of DCT-DWT could be used.

REFERENCES

[1] Y. Xiang, I. Natgunnathan, W. Zhou, G. Belikov T. Zong, "Robust Histogram Shape Based Method for Image Watermarking," in *IEEE Transactions on Circuits and Systems for Video Technology*, 2015, pp. 717-729.

[2] J.H. Connell,R.M. Bolle N.Ratha, "An analysis of minutiae matching strength," in *Audio and video based biometric person authentication*, june 2001, pp. 223-228.

[3] R.R. Manthalkar Baisa L. Gunjal, "An Overview of transform domain robust digital image watermarking algorithms," *Journal of Emerging trends in Computing and Information Sciences*, 2010.

[4] I.Pitas A.G. Bors, "Image Watermarking Using DCT Domain Constraints," in *IEEE International Conference On Image Processing*, 1996, pp. 231-234.

[5] A.Z. Tirkel,C.F. Osborne R.G. Van Schyndel, "A Digital Watermark," in *International Conference in Image Processing*, 1994, pp. 86-90.

[6] Yong Xiang, Iynkaran Natgunanathan Tianrui Zong, "Histogram shape based Robust image Watermarking Method," in *IEEE ICC Communication and Information System Security Symposium*, 2014, pp. 878-883.

[7] Agya Mishra Akhil Pratap Singh, "Wavelet based watermarking on digital image," *Indian Journal of Computer Science and engineering*, 2011.

[8] Shanti Swami Pratibha Sharma, "Digital Image Watermarking Using 3-level Discrete Wavelet Transfrom ," in *Conference on Advances in Communication and Control Systems 2013*, 2013.

[9] S.Esakkirajan, T.Veerakumar S.Jayaraman, *Digital Image Processing*. New Delhi: Tata McGraw Hill, 2009.

[10] Hyoung Joong Kim, Jiwu Huang Shijun Xiang, "Invariant Image watermarking based on statistical Features in the low frequency domain," in *IEEE transaction on circuits and system for video technology* , june 2008, pp. 777-790.