ROBUST WATERMARKING TECHNIQUE USING DIFFERENT WAVELET DECOMPOSITION LEVELS FOR SIGNATURE IMAGE PROTECTION

[1]Rohit Thanki, [2]Ved Vyas Dwivedi & [3]Komal Borisagar
[1&2] Faculty of Technology & Engineering
Chimanlal Ujamshibhai Shah University, Gujarat, India
[3] Atmiya Institute of Technology &
Science, Gujarat, India

rohitthanki9@gmail.com; vedvyasdwivediphd@gmail.com;
krborisagar@aits.edu.in

ABSTRACT

This paper proposed a non-blind watermarking technique based on different wavelet decomposition levels for biometric image protection. In this technique, a biometric image is used as a watermark instead of a standard image, logo or random noise pattern type watermark. For watermark embedding, the original host image and the watermark biometric image are transformed into various levels of wavelet coefficients. The watermark biometric image is embedded into the host image by modifying the values of the wavelet coefficients of the host image using the values of wavelet coefficients of the watermark biometric image. Experimental results demonstrated that the proposed technique was able to withstand various watermarking attacks. The novelty of the proposed technique is that it is used to transform coefficients of the watermark biometric image instead of the Pseudo Noise sequences or any other feature extraction technique.

Keywords: Biometric image, offline signature, watermarking, wavelet decomposition.

INTRODUCTION

The use of the automatic biometric authentication system in various organizations, offices, railway stations, and airports for security purpose is rapidly increasing nowadays. This automatic biometric system can recognize

Received: 2 May 2016 Accepted: 16 November 2016

an individual based on his/her biometric characteristics (Jain & Kumar, 2012). In most of the biometric systems, fingerprint, face, and iris biometric templates are used for biometric recognition. These three biometric characteristics are accepted worldwide and are used widely for individual recognition (Jain & Kumar, 2012). This biometric system has several limitations such as unwanted noise being added to the sensor level, an intra-class variation of biometric traits, the distinctiveness of biometric traits, nonuniversality, and modification or spoof attacks (Jain et al., 2006). Ratha and his research team (Ratha et al., 2001) point out various attack points on a biometric authentication system. These attack points are shown in Figure 1.

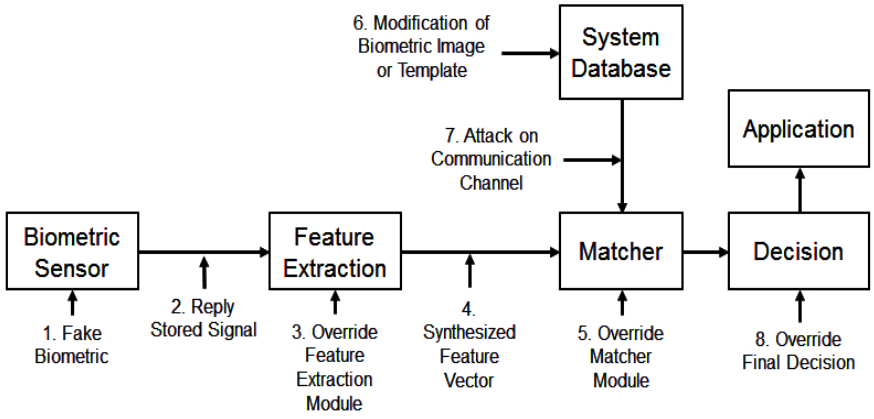


Figure 1. Attack points on a biometric authentication system (taken from Ratha et al., 2001)

In most of the biometric systems, biometric data is vulnerable at the communication channel between two modules of the system. So protection of the biometric data is required at the communication channel when it is transferred from one module to another module. The robust watermarking approach is one of the solutions for the protection of biometric data when it is transferred over the communication channel. Various robust watermarking techniques have been proposed by researchers in the last decade for the protection of biometric data. A few existing watermarking techniques which are related to the proposed watermarking technique are reviewed below.

Inamdar and Rege (2014) proposed a biometric watermarking technique for the protection of multiple biometric images. In this technique, multiple biometric images are used as a watermark for copyright ownership. The speech coefficients which are extracted using LPC, facial features which are

extracted using the Gabor filter, and the signature image are used as watermark information in this technique. This technique stands robust against various watermarking attacks and is used for multiple or single ownership.

Inamdar and her research team (Inamdar et al., 2010) proposed a blind robust biometric watermarking technique for signature image protection. In this technique, PN sequence is embedded into the 2^{nd} level details wavelet coefficients of the host data according to the watermark signature image bits. The authors also described the matching procedure for the signature images. Jundale and Patil (2010) proposed the wavelet-based technique for speech signal protection. In this technique, the speech signal of the individual is taken as the watermark and this watermark is embedded into the wavelet coefficients of the host image.

Mathivadhani and Meena (2010) gave the study of the DCT and the DWT-based watermarking techniques for fingerprint image protection. These techniques are used for the verification of the fingerprint image after the watermarking image. Vatsa and his research team (2009) gave a watermarking technique for voice and facial features protection. This technique is based on the redundant DWT and the phase congruency model. Noore et al. (2007) gave a DWT the based watermarking technique for face image protection. In this technique, facial features and the corresponding text information of the individual are taken as watermark and this watermark information is embedded into the wavelet coefficients of a host fingerprint image. Vatsa and his research team (2006) gave the last significant bit (LSB) and the DWT-based watermarking technique for facial protection. In this technique, the watermark facial features are embedded into the LSB of the wavelet coefficients of a host fingerprint image.

All these existing watermarking techniques are robust against manipulations and provide security to biometric data at a non-secure communication channel in the biometric system. In all these techniques, the host data or image is modified according to the Pseudo Noise (PN) sequence or the watermark biometric features bit. Many existing watermarking techniques are based on the additive or multiplicative watermarking approach. This standard watermarking approach is easily available in the market. So, watermark biometric features can be easily extracted from watermarked data if the imposter applied one of these standard approaches. In the existing watermarking techniques, the wavelet transform is applied to the host image and chooses only one or more than one subband of detail wavelet coefficients for watermark embedding. Also, a few watermarking techniques are available for the protection of the signature image.

In this paper, watermark biometric data such as the signature of the individual is converted into its wavelet coefficients before embedding. These wavelet coefficients of a watermark signature image are embedded into a different level of wavelet coefficients of the host image. Here, all subbands such as approximation and detail wavelet coefficients of the host image are modified according to the respective subbands of the watermark signature image.

The rest of the paper is organized follow. The next section describes the existing watermarking techniques. Then a discussion on the proposed watermarking technique is given. Then the experimental results and a discussion of the results are given. The final conclusion of the paper is given.

EXISTING REFERENCE WATERMARKING TECHNIQUES

There are two reference watermarking techniques available in the literature. Inamdar and her research team (2010) introduced a robust biometric watermarking technique in which they embedded PN sequences according to the signature image bit into high frequency wavelet coefficients (Figure 2).

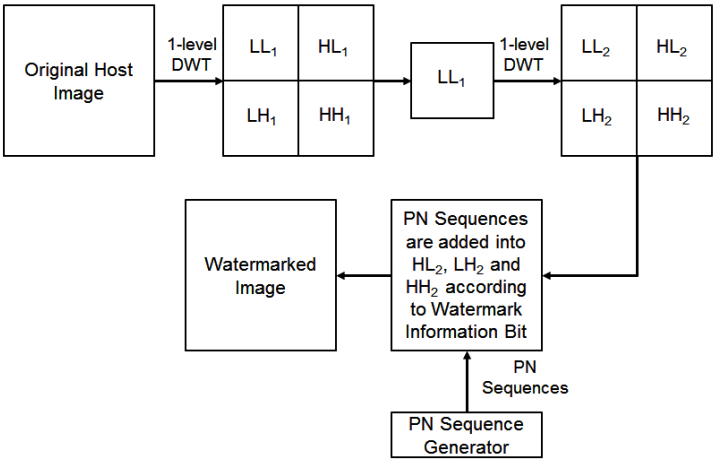


Figure 2. Block diagram of Inamdar et al.'s Reference Watermarking technique (Inamdar et al., 2010).

For watermark embedding purposes, the grayscale host image was decomposed using a single level Discrete Wavelet Transform (DWT). For the second level wavelet decomposition, LL1 was chosen and again the single level DWT was applied on it. Hence the different wavelet sub-bands such as LL2, LH2,

HL2, and HH2 were obtained. The signature image as watermark used by the authors was a binary watermark image which was converted into a binary code. The values of LH2, HL2 and HH2 were modified by PN sequences which were added according to the watermark bits. The main drawback of this technique was that, for the embedding procedure, three different PN sequences were required to generate three detail wavelet sub-bands.

The watermark embedding procedure is given below:

- If the watermark bit contains bit 0 then PN sequences are added using the procedure below:
- If the watermark bit is embedded in one sub-band then

$$HL_2 = HL_2 + \alpha \times PN\_Sequence\_1 \quad (1)$$

- If the watermark bit is embedded in two sub-bands then

$$LH_2 = LH_2 + \alpha \times PN\_Sequence\_2 \quad (2)$$

- If the watermark bit is embedded in all three sub-bands then

$$HH_2 = HH_2 + \alpha \times PN\_Sequence\_3 \quad (3)$$

- If the watermark bit contains bit 1, then coefficients of all the three sub-bands are not modified.

The watermark information can be extracted using the correlation between coefficients of wavelet sub-bands and PN sequences at the extraction side. The watermark extraction procedure is given as follow:

- The correlation between the PN sequence and its corresponding wavelet sub-band coefficients is calculated and stored as a sequence which is equal to the size of the watermark information.

$$Correlation\_HL_2 = corr2(HL_2, PN\_Sequence\_1) \quad (4)$$

- If the watermark bit is embedded in two sub-bands then

$$Correlation\_LH_2 = corr2(LH_2, PN\_Sequence\_2) \quad (5)$$

- If the watermark bit is embedded in all three sub-bands then

$$Correlation\_HH_2 = corr2(HH_2, PN\_Sequence\_3) \quad (6)$$

- When the watermark bit is embedded in more than one sub-band, then find the average of the correlation sequences. Then the standard deviation of these sequences is found and then the correlation is compared with the value of the standard deviation to decide the watermark bit.

- If correlation > std (x) then set the watermark bit value set to zero, otherwise set the watermark bit value set to one.
- Then reshape the watermark bit sequence to generate the original watermark information at the detector side.

Another reference watermarking technique was given by the same authors (Inamdar & Rege, 2014) in which the authors embedded more than one watermark biometric information in different wavelet coefficients of the host image. In this technique, the authors proposed watermarking techniques for multiple biometric data which embeds visible and invisible watermark biometric information.

The authors described that PN sequences do not have any information about individuals. Therefore, the authors used various biometric features such as voice, face, and signature as watermark information depending on the owner is characteristics. This technique was based on the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT) decomposition. In this technique, information watermark information biometric was embedded invisibly in various wavelet sub-bands of the host image, and one watermark biometric information was embedded visibly in the DCT coefficients of the watermarked image where two biometric images were already embedded. The multiple watermark biometric is embedded as depicted in Figure 3.

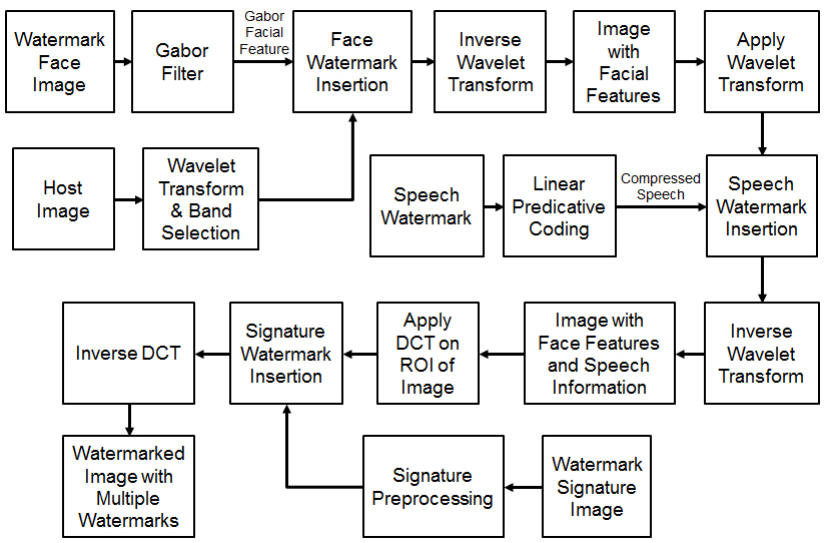


Figure 3. Block diagram of the Inamdar and Rege Reference Watermarking technique (Inamdar & Rege, 2014).

The watermark embedding procedure is given below:

- Take a face image as watermark. Then apply the Gabor filter on it to extract the facial features of the user.
- Take a host image and apply wavelet transform on it to convert it into various sub-bands of wavelet coefficients. Then chose one sub-band of the wavelet coefficients of the host image where the Gabor facial features are inserted to get a watermarked image with facial features.
- Take a speech of the user as watermark and apply the Linear Predicative Coding (LPC) on it to get compressed speech features of the user.
- Then apply wavelet transform on the watermarked image and get various sub-bands of wavelet coefficients of the watermarked image.
- The compressed speech features are inserted into one sub-band of the wavelet coefficients of the watermarked image to get a watermarked image with facial features and speech information.
- Take the signature of the user as a watermark which is embedded visibly in the watermarked image which has facial features and speech information.
- For watermark signature embedding, apply the Discrete Cosine Transform (DCT) on ROI of the watermarked image which has the facial features and speech information to get the DCT coefficients of the watermarked image.
- Then the watermark signature is embedded into the DCT coefficients of the watermarked image. Apply the inverse DCT on the modified DCT coefficients to get the final version of the watermarked image.
- The final version of the watermarked image has the invisible facial features and speech information with visible signature on it.

These two reference watermarking techniques are used for signature image protection. In the first reference model, the Pseudo Noise (PN) sequences are required for watermark information. These PN sequences do not have any significant information about the individual. In the second reference model, various transforms such as DCT and DWT, two additional procedures such as the Gabor filter and the Linear Predicative Coding (LPC) for feature extraction of the watermark biometric are required. Also, the payload capacity of these reference watermarking techniques is less than 50%. These are the major reasons which motivated us to propose this biometric watermarking technique.

This proposed watermarking technique provides protection to the biometric image without using of any additional technique such as feature extraction. The reason behind not using additional technique in this proposed technique is that

we have used wavelet coefficients of the watermark biometric image instead of the actual value of the watermark biometric image. Also, the payload capacity of the proposed technique can achieve 100%. In this proposed technique, watermark biometric image is embedded into the same size of the host color image which is not possible in many existing watermarking techniques.

PROPOSED WATERMARKING TECHNIQUE

In this paper, we have proposed a watermarking technique which embeds biometric watermark image into the host image. This proposed watermarking technique can be used for any type of biometric image.

We have proposed a wavelet based technique where strategy wise wavelet coefficients of biometric watermark information are embedded into corresponding wavelet coefficients of the host image. This proposed technique is non-blind watermarking technique because the original host image is required for extraction of the biometric watermark information. The watermarking technique is proposed here as it is possible for equal size of watermark information to be embedded into the host image which is not possible in existing wavelet based watermarking techniques available in the literature. The block diagram of the proposed watermarking technique is given in Figure 4. The proposed watermarking technique is formulated as follows:

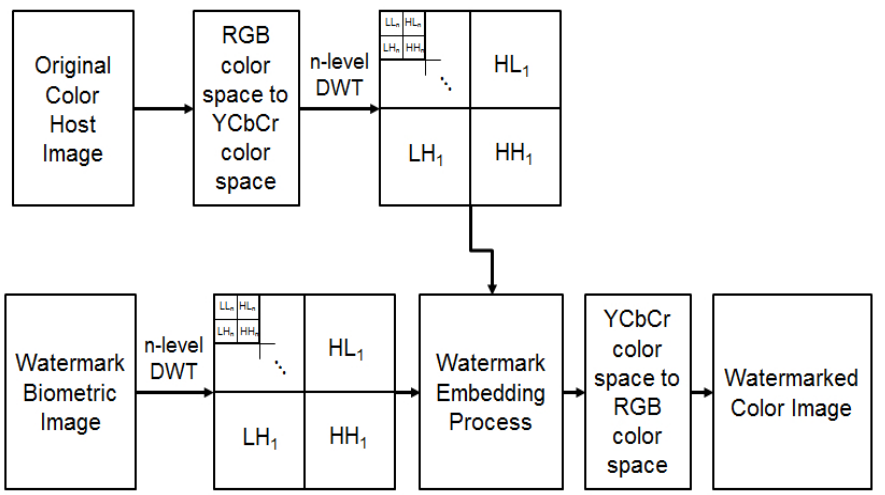


Figure 4. Block diagram of the proposed watermarking technique.

Watermark Embedding Process

The algorithm for watermark embedding is shown in Figure 5. The following steps are used for watermark embedding.

- Take a host color image and convert it from RGB color space to YCbCr color space. The reason behind the color space conversion is that when any compression is applied to any color image than the RGB color space it is more affected compared to the YCbCr color space. YCbCr color space requires less storage compared to the RGB color space.
- Take a watermark biometric image with an equal size of the host color image. Then the watermark signature image is embedded in the Y plane of host image as shown in the procedure below.

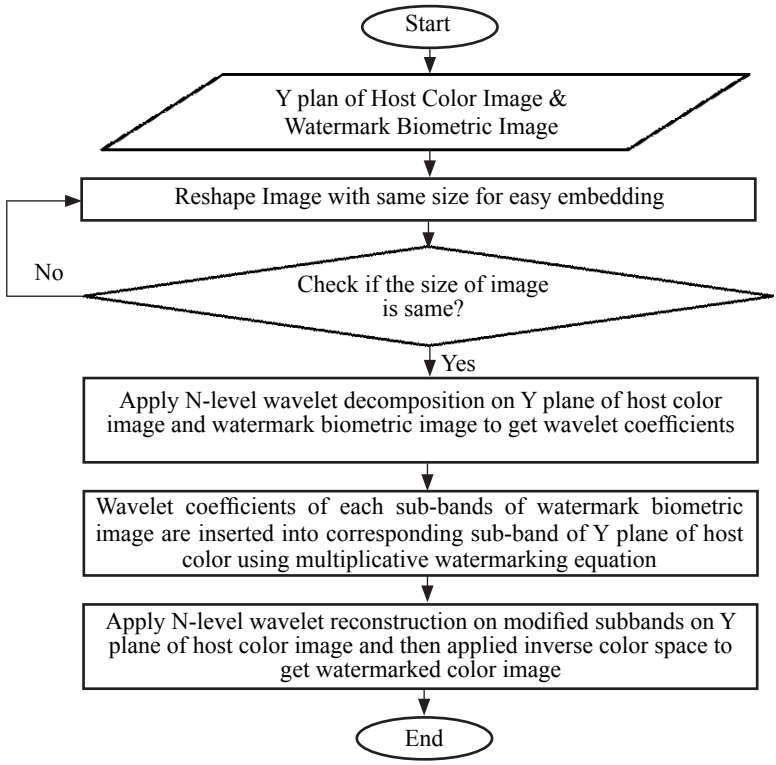


Figure 5. Watermark embedding process algorithm.

Watermark Extraction Process

The algorithm for watermark extraction is shown in Figure 6. The following steps are used for watermark extraction.

- Take a watermarked color image and convert it from RGB color space to YCbCr color space. Then the watermark biometric image is extracted from the Y plane of the watermarked color image as shown in the procedure below.

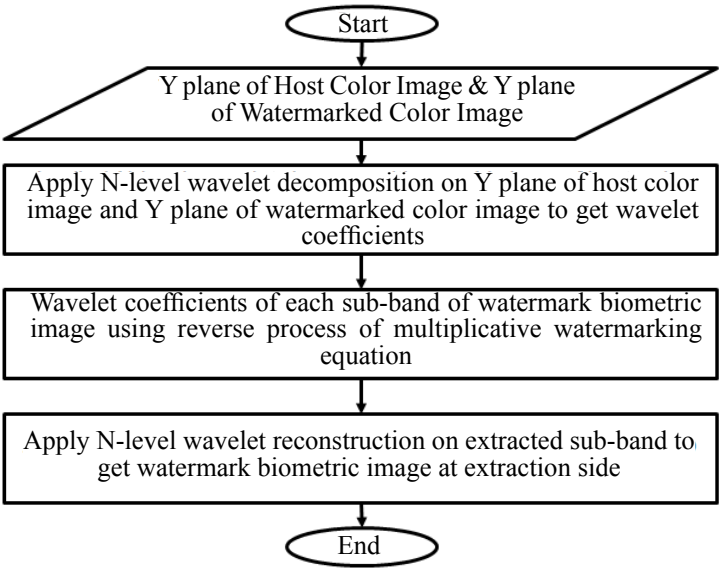


Figure 6. Watermark extraction process algorithm.

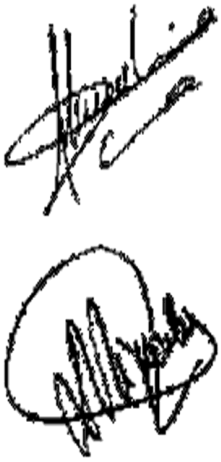
RESULTS

In order to test the performance of the proposed watermarking technique, the MATLAB platform was used and a number of experiments were performed on different host color images. What is necessary for the proposed watermarking technique is that the size of the watermark biometric image and the host color image must be same. This proposed technique can be used for any type of biometric image. Here, we took the signature image of an individual for the experiment.

The host color images with 512×512 pixels such as Lady, Peppers are shown in Figure 7(a). Two binary signature images with 512×512 pixels are used as watermark biometric images which are shown in Figure 7(b). The signature image 1 is embedded into the Lady image and signature image 2 is embedded into the Peppers image. We took big images for a proper representation of the

results. This technique can be used for any size of the watermark biometric image and the host image but the condition is that the size of both images must be the same.

(a) Lady Color Image and Peppers Color Image taken as Host Images



(b) Original Signature Images as Watermark Images

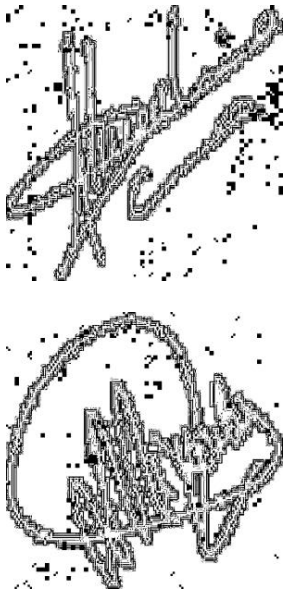
Figure 7. Test images.

We applied up to the 3rd level wavelet decomposition on the Y plane of the host color image and the watermark signature image for generating watermarked color images. For watermark embedding, the gain factor k was set to 500. The watermark signature image can be extracted from the watermarked color image using the watermark extraction procedure which is described in the previous section. Figure 8(a) shows the resultant watermarked color images. The resultant images show no perceptual degradation in the watermarked color images according to HVS. Figure 8(b) shows the extracted signature watermarked image from the watermarked Lady and Peppers images respectively.

In order to check the robustness of the proposed watermarking technique, the watermarked images were attacked by various watermarking attacks such as Median, Mean and Gaussian low pass filtering, Gaussian noise addition, Salt & Pepper noise addition, Speckle noise addition, JPEG Compression,

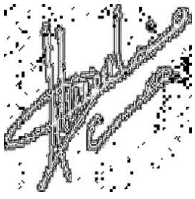
Histogram Equalization, Rotation, and Cropping. After applying these attacks on the watermarked images, the extracted signature watermark images were compared with the original signature watermark images. Figure 9 shows the resultant watermarked color images and the extracted signature watermark images after the watermarking attacks.

(a) Watermarked Color Images

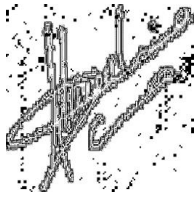


(b) Extracted Watermark Signature Images

Figure 8. Watermarked images and extracted signature watermark images.



(a) JPEG Compression (80:1)

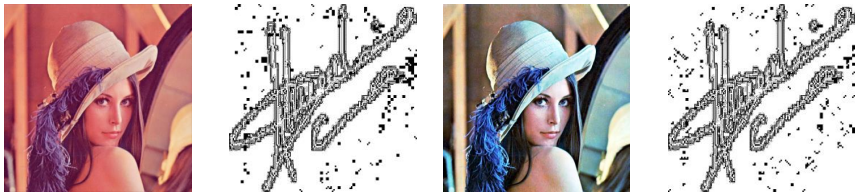


(b) JPEG Compression (70:1)

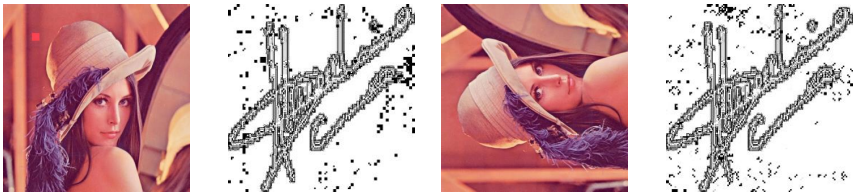
(continued)

(c) Addition of Gaussian Noise (d) Addition of Salt & Pepper Noise

(e) Addition of Speckle Noise (f) 3×3 Median Filtering



(g) 3×3 Gaussian Low Pass Filtering (h) Histogram Equalization



(i) Cropping (j) Rotation

Figure 9. Watermarked images and extracted watermark signature images after application of various watermarking attacks.

Quality measures such as Peak Signal to Noise Ratio (PSNR) and Structural Similarity Measure Index (SSIM) were used for checking imperceptibility and

robustness of the proposed technique. These two characteristics are a basic requirement of any watermarking algorithm (Olanweraju et al., 2009).

The quality measure such as PSNR (Petitcolas, 2000; Olanweraju et al., 2009) was used to measure the quality of the host color image and its watermarked version. The corresponding PSNR values for the watermarked image after the application of various watermarking attacks are given in Table 1. PSNR is used to measure the difference between a host color image and its watermarked version at the embedder side (Petitcolas, 2000; Olanweraju et al., 2009). The PSNR values of the test watermarked color images shown in Table 1 indicate that this proposed watermarking technique can provide imperceptibility of embedded watermark signature image against watermarking attacks such as compression, the addition of noise, various filtering, cropping, histogram equalization, and rotation

.

Table 1

PSNR Values of Test Watermarked Images after Application of Various Watermarking Attacks

Attacks	Lady image	Peppers image
No attack	51.95	52.52
JPEG compression (80:1)	44.10	42.99
JPEG compression (70:1)	43.17	42.01
Addition of Gaussian noise (μ= 0, σ = 0.001)	29.51	30.07
Addition of Salt & Pepper noise (Variance = 0.005)	27.86	27.95
Addition of speckle noise (Variance = 0.004)	29.50	31.31
Median filtering (3×3)	35.47	36.92
Mean filtering (3×3)	31.72	31.00
Gaussian low pass filtering (3×3)	40.77	40.16
Histogram equalization	14.38	19.15
Cropping	53.46	11.17
Rotation (90°)	11.54	48.90

The quality measure such as SSIM (Wang & Bovik, 2002) was used to measure the quality of the watermark signature image and its extracted version. The corresponding SSIM values for the extracted watermark signature image after the application of various watermarking attacks are given in Table 2. The SSIM value of the extracted watermark signature images shown in Table 2 indicate that the performance of the proposed watermarking technique can be

changed under the influence of various watermarking attacks. This indicate that this proposed watermarking technique provides robustness to watermark signature images against various watermarking attacks.

Table 2

SSIM Values of Extracted Signature Watermark Images after Application of Various Watermarking Attacks

Attacks	Lady image	Peppers image
No attack	0.895	0.856
JPEG compression (80:1)	0.891	0.857
JPEG compression (70:1)	0.890	0.857
Addition of Gaussian noise (μ= 0, σ = 0.001)	0.908	0.865
Addition of Salt & Pepper noise (Variance = 0.005)	0.901	0.861
Addition of Speckle noise (Variance = 0.004)	0.910	0.864
Median filtering (3×3)	0.883	0.854
Mean filtering (3×3)	0.884	0.853
Gaussian low pass filtering (3×3)	0.892	0.856
Histogram equalization	0.890	0.860
Cropping	0.890	0.857
Rotation (90°)	0.894	0.857

We also checked the robustness of the proposed watermarking technique against ambiguity attacks which are also known as confusion attacks (Bhatnagar & Balasubramanian, 2009; Kejariwal, 2003). In this attack, the imposter attempts to confuse by generating fake watermark data. The imposter tries to generate fake watermark biometric data and a host data where the watermark biometric data is embedded.

Our proposed watermarking technique provides protection to the watermark signature image against ambiguity attacks. If the watermarked image is available in the public domain, and the imposter can try to extract a signature image from the watermarked image. Then the imposter needs to get the level of wavelet decomposition and then needs the wavelet coefficients of the various sub-bands for generate a watermarked image. The imposter tries to extract a watermark signature image form a watermarked image using all the sub-bands but without knowledge of the gain factor, the imposter cannot generate the watermarked image. The gain factor is used as the secret key in this proposed watermarking technique. The gain factor is only known to an

authorized individual. The gain factor is any positive number and selection of the gain factor depends on the authorized individual who wants to protect his / her biometric image. So the proposed watermarking technique can stand with ambiguity attack.

This proposed watermarking technique's comparison with existing watermarking techniques available in literature with various parameters is summarized in Table 3. In this proposed watermarking technique, all four sub-bands of the various levels of the wavelet coefficients are used for watermark embedding. In the existing watermarking technique, the2nd level detail wavelet coefficients are used for watermark embedding.

Table 3

Comparison of Proposed Watermarking Technique with Existed Watermarking Technique available in Literature

Features & parameters	Type of watermarking technique	No. of biometric watermark used	Additional techniques for biometric watermark feature extraction	Used wavelet coefficients of host image for watermark embedding	Information used for watermark embedding	PSNR (dB)
Inamdar et al.'s technique (2010)	Robust	One	PN Sequence generation	2-level sub-bands of detail wavelet coefficients	PN sequences are embedded into coefficients of host image according to watermark biometric bits	40.92
Proposed watermarking technique	Robust	One	Not required	N-level sub-bands of all four wavelet coefficients	Wavelet coefficients of watermark biometric image	52.00

In existing watermarking techniques, PN sequences use signature watermark extraction for watermark embedding. In the proposed watermarking technique, wavelet coefficients of the signature watermark are used for watermark embedding. In existing watermarking techniques, additional techniques are used for biometric watermark feature extraction. But in this proposed watermarking technique, an additional technique is not required because here we have used wavelet coefficients of watermark biometric image which represent images in various frequencies. The PSNR value of the proposed watermarking technique achieved is higher than the existing watermarking technique available in the literature.

CONCLUSION

A non-blind watermarking technique is proposed in which wavelet coefficients are used instead of a PN sequence or biometric features. The embedding is done by modifying wavelet coefficients of the host image with the wavelet coefficients of the watermark signature image. This technique is robust against various watermark attacks. This proposed technique is also robust and stands ambiguity attacks. The observations below are made for this proposed watermarking technique.

The technique is purely based on wavelet transform where wavelet coefficients of the host and the watermark image are utilized. This technique does not require any additional technique for watermark signature image embedding. The security of the proposed watermarking technique depends on the wavelet coefficients of the host and the watermark images. In the proposed technique, wavelet coefficients of the host color image and the watermark signature image are utilized which provide additional security to the watermark signature image. This technique provides 100% payload capacity which is not available in many existing wavelet-based existing watermarking technique. This technique provides high quality measure compared to existing watermarking techniques available in the literature.

REFERENCES

Bhatnagar, G., & Raman, B. (2009). A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces*, *31*(5), 1002-1013.

Inamdar, V. S., & Rege, P. P. (2014). Dual watermarking technique with multiple biometric watermarks. *Sadhana*, *39*(1), 3-26.

Inamdar, V., Rege, P., & Arya, M. (2010). Offline handwritten signature-based blind biometric watermarking and authentication technique using biorthogonal wavelet transform. *International Journal of Computer Applications*, *11*(1), 19-27.

Jain, A. K., & Kumar, A. (2012). Biometric recognition: An overview. In *Second generation biometrics: The ethical, legal and social context* (pp. 49-79). Springer Netherlands.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *Information Forensics and Security, IEEE Transactions on*, *1*(2), 125-143.

Jundale, V., & Patil, S. (2010). Biometric speech watermarking technique in images using wavelet transform. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, 33-39.

Kejariwal, A. (2003). Watermarking. *Potentials IEEE, 22*(4), 37-40.

Mathivadhani, D., & Meena, C. (2010). A comparative study of fingerprint protection using watermarking techniques. *Global Journal of Computer Science and Technology, 9*(5), 98-102.

Noore, A., Singh, R., Vatsa, M., & Houck, M. M. (2007). Enhancing security of fingerprints through contextual biometric watermarking. *Forensic Science International*, *169*(2), 188-194.

Olanweraju, R. F., Aburas, A. A., Omran, O., & Abdalla, A. H. H. (2010). Damageless digital watermarking using complex-valued artificial neural network. *Journal of Information and Communication Technology,* 9, 111-137.

Petitcolas, F. A. (2000). Watermarking schemes evaluation. *Signal Processing Magazine, IEEE*, *17*(5), 58-64.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614-634.

Shih, F. Y. (2007). *Digital watermarking and steganography: Fundamentals and techniques*. CRC Press.

Vatsa, M., Singh, R., & Noore, A. (2009). Feature-based RDWT watermarking for multimodal biometric system. *Image and Vision Computing*, *27*(3), 293-304.

Vatsa, M., Singh, R., Noore, A., Houck, M. M., & Morris, K. (2006). Robust biometric image watermarking for fingerprint and face template protection. *IEICE Electronics Express*, *3*(2), 23-28.

Wang, Z., & Bovik, A. C. (2002). A universal image quality index. *Signal Processing Letters, IEEE*, *9*(3), 81-84.