Role of watermarking in securing the Biometric Signature Database

Jyotika Chopra1†, Amod Kumar2††, Anupma Marwaha3†††and Sanjay Marwaha4††††

Research Scholar, SLIET Longowal

Summary
In this paper, a robust watermarking scheme is proposed for signature biometric. Conventional frequency domain algorithms use complex calculations but the proposed work avoids such calculations by using simple yet robust XOR operation. Experiments were done on freely available signature database as well as on standard images. Results show that the encrypted (proposed) watermark is invisible and secure with respect to various geometric operations such as rotation, dilation, Gaussian noise, alpha transparency and circular shift which may be attempted by the intruders. The proposed approach achieves large values of Peak Signal to Noise Ratio (PSNR) which ensures the watermark imperceptibility. High value of Number of Pixel Change Rate (NPCR) confirms the security. The proposed technique, thus, outperforms the existing methods and is resistant towards various attacks.

Keywords:
watermark, security; copyright; peak signal to noise ratio (PSNR); Number of pixel Change Rate (NPCR).

1. Introduction

Using internet on smart phones and in business through public networks makes the user's data insecure. Many digital watermarking methods have been proposed for different purposes such as copyright protection, ownership verification etc. thus, preventing the unauthorized distribution. Digital watermarking is the process of embedding digital information in a digital content. Watermarking systems insert data in such a way that the signal quality is preserved. There are three design properties a good watermark process must possess: imperceptibility, robustness and data payload which have conflict with each other [1]. The imperceptibility of the watermark indicates its transparency property. Robustness is the ability of the technique to successfully extract the watermark without being degraded or destroyed by attacks applied to the watermarked content. Researchers have tried many techniques, both in spatial and frequency domain, to embed watermark in different digital contents. In 1999, authors in [2] used Discrete Wavelet Transform (DWT) for watermark of still images but it was observed that parametric analysis of the models could be highly inaccurate in estimating a wide range of image transformations and costly to implement for large images. In 2002, [3] introduced a simple scheme to provide security to fragile authentication watermark. It gave information about cropped area and localized pixel position only if larger blocks were used. In this process, first the image was divided into 8 x 16 blocks and then hash was calculated for the 7 MSB's of the corresponding blocks. XOR was done with the Hash and with the equivalent binary logo block which was embedded and inserted in the LSB in such a way that when the attacker tried to make a change to the authenticated image, it will not be detected. In [4], Kim proposed Zernike moments for robust watermarking systems by modifying the vector of the systems. However, it suffered difficulty in implementation and to reconstruct the watermark image besides being time consuming.

This process was only possible with the Zernike polynomial by increasing intensity of pixels. The root mean square error was the method used for checking the similarity between the images. Zernike gave good performance against JPEG compression, scaling and rotation. However, rotations with larger angle produced more failure in detection than smaller angles. In 2010, [5] proposed multi-resolution wavelet decomposition for watermarking by quantized steps with key. Though the proposed technique ensured an invisible watermark and was robust to attacks, the quality of the watermark image decreased from increase in quantization steps. Lin et al in [6] suggested Spatial Domain Watermarking (SDW) scheme based on quantization, which provided acceptable watermarking capacity and computational complexity. In 2012, Bhatnagar et al [7] proposed fractional wavelet packet transform watermarking scheme to decompose an image. The watermark image was created by modifying the frequency positions that were stored in key which only the owner knew. The optimal value of transform order was obtained by trial-and-error algorithm, but it was not used in watermark extraction because it increased the complexity of the system. In [8], authors applied watermarking using Discrete Cosine Transform (DCT). Structural similarity index was used with DCT for faster implementation. The image quality reduced due to disparity between adjacent blocks. In 2014, Zhu et al [1] introduced a normalized correlation based on quantization modulation technique for watermarking. The operations were not performed on host signals but on the feature signal transformed from host signal. This process was unique and caused complexity in mapping. In 2016, Abdelhakim et al [9] applied DCT with fitness function for watermark. Although fitness function provided better

Manuscript received November 5, 2025
Manuscript revised November 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.11.11

compromise between imperceptibility and robustness, it could not be used for improving watermark insertion parameters for each watermark bit separately using traditional metrics. In 2017, Sulong et al [10] reported a hybrid domain for watermarking. The scheme used was robust to image compression (JPEG), image editing, cropping and salt & pepper noise. However, it was fragile against Gaussian noise and geometric distortions. The system failed against Salt & Pepper (0.03%) attack and Sharpening attack as it could not attain the acceptance value of 30 for PSNR which is required for perceptual fidelity. In 1998, Pitas [11] described a novel method based on statistical and chaotic views for watermarking. The position of pixel did not change when the watermarking was in process. The whole procedure of moving a pixel was insensitive to image distortion, so detection algorithm was not able to calculate the pixel position. In 2015, Hoang et al [12] proposed a novel gait authentication scheme on mobile phone. This scheme was resistant to certain attacks. However, in real-valued patterns, the Euclidean distance of intra and inter-class patterns was near to the ground and their distribution areas overlapped. By using a proper threshold, these patterns were recognized. In 1998, Wong [13] announced a watermarking scheme for image integrity and owner verification. In this process, LSB was set to zero. MD5 (Message digest) was considered as hash function and was calculated for each block and XOR operation was performed on it. This process was conscious about changes that were made to modify the watermark and this process was used for protecting visible watermark also by introducing contrast density control parameter λ whose range was between 0 and 1.

In this paper, focus was to propose a technique which ensured security with less computational complexity. A novel secure watermarking scheme was developed which is based on the 1D key that acts as a security key for encryption and decryption of watermark. For the validation of the proposed technique, freely available databases from www.gpds.ulpgc.es/download have been used [14]. For conducting experiments, 480 color signatures of size 334 x 1082 pixels with 24 genuine signature images of first 20 subjects were taken from the dataset. We examined this watermark scheme based on its main properties - robustness, security and imperceptibility - on the basis of values of image quality parameters under various signal processing and geometrical attacks.

This paper is organized as follows. Section 2 describes proposed watermarking scheme. Section 3 describes the pseudo code for proposed methodology of watermark insertion, extractions etc. In Section 4, performance analysis is done with the help of image quality parameters. Section 5 reports the experimental results on image quality parameters. Discussions on proposed technique are done in section 6 and Section 7 concludes the paper.

2. Proposed Watermarking Scheme

The three major steps of watermarking are: embedding, modification by attacks and extraction. Primarily, a signature is taken as input (I_k) and is chosen from the freely available database. We have used a color watermark of size 90 x 90 pixels (Fig. 1), which is converted first into a gray-scale image and further into sequence vector map.

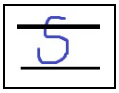

Fig. 1: Watermark

The input signature image and gray-scale watermark can be put mathematically as Eq. (1) and Eq. (2), respectively.

$$I_{SIG} = \lfloor i_{pq} \rfloor_{P \times Q} \quad (1)$$

$$I_{WM} = [a_{mn}]_{M \times N} \quad (2)$$

Column sequence vectors are obtained from

$$C = [C_1 \quad C_2 \quad C_3 \quad C_4 \quad \cdots \quad C_n]$$

where C_i = i^{th} column vector of I_{WM}. A user defined chunk value ($C_{\min}$) is used to insert the watermark at chunk locations (C_i). In input signature, I_{SIG}, the position of insertion is always the multiple of chunk value ($C_{\min}$). The chunk locations are expressed in Eq. (3), where L is the highest integer such that $LC_{\min} < P$ where P indicates row size of I_{SIG}.

$$C_{NK} = [C_{\min} \quad 2C_{\min} \quad \cdots \quad LC_{\min}] \quad (3)$$

Then process of XOR operation between elements of locations of I_{SIG} indicated by C_{NK} and the elements of I_{WM} is carried out for all the rows of I_{SIG} keeping other elements of I_{SIG} intact. This gives an encrypted image E_I.

3. Pseudo code for Proposed Watermark Scheme

In this section, pseudo code for watermark insertion and extraction is given in Fig 2 and Fig 3.

PSEUDO CODE FOR WATERMARK INSERTION PROCESS

STEP1: Pick one signature, I_k from Database and watermark of size 90 x 90
STEP2: Convert Watermark RGB into gray scale
STEP3: Convert 2-D into sequential vector map, C_{SV} (i).
STEP4: Obtain Security Key and get index values from sequential map
STEP5: Choose any Chunk location, C_i
STEP6: Calculate another chunk location, C_{min} which is always the multiple of C_i
STEP7: Check C_i% C_{min} ==0
STEP8: If yes,

$$E_I = C_{SV}(i) \otimes I_k(n, m \times C_i)$$

STEP 9: If no, go to STEP 1 then to STEP 6
STEP10: Watermark is embedded on image.

Fig. 2: Pseudo code for Watermark Insertion

PSEUDO CODE FOR WATERMARK EXTRACTION PROCESS

STEP1: Pick one watermarked signature, I_{Wk} from database and watermark of size 90 x 90
STEP2: Convert Watermark into gray scale
STEP3: Convert 2-D into sequential vector map, C_{SV} (i)
STEP4: Obtain Security Key and get index values from sequential map
STEP5: Choose any Chunk location, Ci
STEP6: Calculate another chunk location, C_{min} ,which is always the multiple of C_i
STEP7: Check C_i% C_{min} =0
STEP8: If yes,

$$E = C_{SV}(i) \otimes I_{Wk}(n, m \times C_i)$$

STEP 9: If no, go to STEP 1 then go to STEP 6
STEP10: Watermark is extracted from image.

Fig. 3: Pseudo code for Watermark Extraction

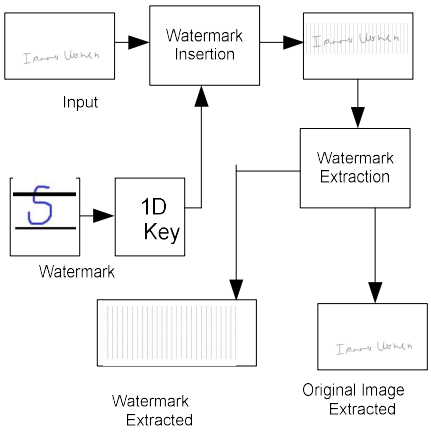

Fig. 4: Block Diagram of Proposed Watermark Process

4. Performance Analysis

The performance of system can be measured using following image quality parameters:

4.1 Peak signal to noise ratio (PSNR):

It is used to calculate the watermark imperceptibility after embedding in image. PSNR is computed between Input image I_k and watermarked image E_I, for checking the image degradation after embedding a watermark, using Eq (4)

$$PSNR_1 = 10\log_{10}\left(\frac{\max\left(\max\left(I_k(i,j) - E_I(i,j)\right)\right)^2}{MSE}\right) dB \quad (4)$$

The acceptable range of PSNR is 38dB [15].

Mean Square Error (MSE) in the above equation is defined using Eq. (5):

$$MSE = \frac{1}{P \times Q}\sum_{i=1}^{P}\sum_{j=1}^{Q}\left(I_k(i.j) - E_I(i,j)\right)^2 \quad (5)$$

4.2. Number of Pixel Change Rate:

To measure the security of watermarked image against attacks to alter the watermark, Number of Pixel Change Rate (NPCR) is calculated. It calculates the change in number of pixel between watermark image and attacked watermark image using Eq. (6). The higher value of NPCR indicates higher resistance to attacks which depicts higher image security. For images E_I (i, j) and E_{IA}

(i, j) having difference of one pixel which is indicated by output S(i, j).

$$\left[\begin{array}{l} E_I(i,j) = E_{IA}{}'(i,j)\ then\ S(i,j) = 1 \\ E_I(i,j) \neq E_{IA}{}'(i,j)\ then\ S(i,j) = o \end{array}\right] \quad (6)$$

$$NPCR = \frac{S(i,j)}{PxQ} * 100$$

where P and Q are the rows and columns of the image.

5. Evaluation of proposed technique

To evaluate the performance of the proposed technique, signal and geometrical attacks are considered: Rotation attack by -0.1° to -1.5°, -90° to -360°; Dilation, Gaussian range of noise density varying from 0.0001 to 0.0005; 0.001 to 0.005; 0.01 to 0.05; alpha transparency by 0.5 and Circular shift by 50 degree. Table 1 shows the image quality parameter values for each type of attack. The PSNR tells about the watermark imperceptibility whereas high value of NPCR ensures that proposed technique offers large resistance to attacks which indicates high security to the system.

Table 1: Effect on Performance parameters due to attack on Signature Database

Attack	Variation	NPCR (%) (Watermarked image, watermarked attack image)
Rotation	-0.1°	90.16
	-0.5°	97.20
	-1.0°	85.66
	-1.5°	84.46
	-90°, -270°	41.13
	-180°,	84.20
	-360°	100
Dilation	Sphere,25	93.27
Gaussian	Mean=0, Var=0.0001	54.62
	0.0002	52.21
	0.0003	51.12
	0.0004	51.07
	0.0005	50.64
	0.001	48.98
	0.002	48.16
	0.003	47.81
	0.004	46.82
	0.005	---
	0.01	47.11
	0.02	46.87
	0.03	46.78
	0.04	46.69
	0.05	46.65
Alpha Transparency	0.5	1.23
Circular Shift	50°	85.91

The proposed technique is also compared with other techniques as shown in Table 2. It is also tested on standard image Lena shown in Fig 5 and Baboon in Fig 6.

Fig.5 Lena Image

Fig.6 Baboon Image

Table 2: PSNR Performance due to Gaussian attack

Variation	0.01		0.02		0.03	
Ref	[16]	P	[16]	P	[16]	P
Lena	20.18	58.4235	20.08	58.4235	19.91	58.4235
Baboon	20.10	55.9935	20	55.935	19.82	55.935

*P: Proposed work

6. Discussion on Results

On the input dataset of 480 images, PSNR was calculated between input signature image and its watermarked image. Its value was obtained in the range 38.8 dB to 48.3 dB i.e. more than 38 dB which shows watermark is imperceptible. The discussion on each attack is as below:

6.1 Effect of Rotation:

The watermarked image is rotated in negative range of 0.1° to 1.5° and from 90° to 360°. Such rotation attack was simulated to mimic the truncation errors that degrade the image. It is analyzed that by taking one full complete circular rotation, it will happen twice that the figure will look precisely same but in opposite direction. High value of NPCR obtained between embedded watermark and extracted watermark indicates that system is secure except at 90° and 270°.

6.2 Effect of Dilation:

The Dilation is the complementary to that of erosion operation. If E_I^C is the complementary of image E_I, then dilation of set E_I by a set S, is defined as

$$\mathbf{E_I} \oplus S = \left(\mathbf{E_I}^{C} \oplus S^{C} \right)$$

In this case also, high NPCR ensures that system is secure against dilation attack.

6.3 Effect of Gaussian noise:

The Gaussian noise blurs the image. It can be seen from the result obtained that whenever the noise density increases, the value of NPCR decreases. The Noise density 0.0005 is the threshold value. For values greater than this value, system is insecure.

6.4 Effect of Alpha Transparency:

Alpha transparency is the mixing of image with its background to make the visualization partial or fully transparent. Its range varies from 0 to 1. Adding 0.5 composition in image makes the system insecure that can be seen from the low value of NPCR achieved.

6.5 Effect of Circular shift:

High value of NPCR shows that system resists the circular attack at 50 degree and is, therefore, secure.

7. Conclusions

It is summarized that proposed technique is robust for all the attacks. The attacks fail to alter the watermark in general. In particular, system is secure to circular attack and dilation attack. For Gaussian attack, the system is robust and secure to within its threshold limit. The rotation attacks are robust and secure at all negative angles except 90º and 270º. The system is unsecure for alpha transparency attack. In future, the work shall be extended to more parameters and more attacks in terms of robustness.

Acknowledgments

The authors would like to thank Director, Sant Longowal Institute of Engineering and Technology, Longowal, India for providing opportunity and for extending computational facilities for this work.

This Research did not receive any specific grant from funding agencies in the public, commercial or not-for-profit sectors.

References

[1] Zhu, X., Ding, J., Dong, H., Hu, K., and Zhang, X. (2014), Normalized correlation-based quantization modulation for robust watermarking. *IEEE Trans. Multimed*., 16(7): 1888–1904.

[2] Kundur, D., and Hatzinakos, D. (1999), Digital watermarking for telltale tamper proofing and authentication. *Proc. IEEE*, 87(7) :1167–1180.

[3] Fridrich, J, Security of Fragile Authentication Watermarks with Localization (2002), *Security and Watermarking of Multimedia Contents IV, Edward J. Delp III, Ping Wah Wong, Editors, Proceedings of SPIE* Vol. 4675:691-700.

[4] Kim, H.S., and Lee, H.K. (2003), Invariant Image Watermark Using Zernike Moments. *IEEE Trans. Circuits Syst. Video Technol*., 13(8): 766–775.

[5] Preda, R.O and Vizireanu D.N. (2010), A robust digital watermarking scheme for video copyright protection in the wavelet domain. *Measurement*, 43(10): 1720–1726.

[6] Lin, Y.-T., Huang, C.-Y., and Lee, G.C. (2011), Rotation, scaling, and translation resilient watermarking for images. *IET Image Process.,* 5(4): 328-340.

[7] Bhatnagar, G., Raman, B, and Wu, Q.M.J (2012), Robust watermarking using fractional wavelet packets transform. *Image Process. IET*, 6(4): 386–397.

[8] Golestani, H.B., and Ghanbari M. (2013), Minimisation of image watermarking side effects through subjective optimisation. *IET Image Process*, 7 (8): 733–741.

[9] Abdelhakim, A.M., Nassar, A.M., and Saleh, H.I. (2016), Quality metric-based fitness functions for robust watermarking optimisation with Bees algorithm. *IET Image Process*, 10 (3): 247–252.

[10] Sulong, G. Bin, Hasan, H, Selamat, A, and Ibrahim M. (2012), A New Color Image Watermarking Technique Using Hybrid Domain. *International Journal of Computer Science Issues,* 9(1): 109-114

[11] Pitas, I. (1998), A method for watermark casting on digital images. *IEEE Trans. Circuits Syst. Video Technol.,* 8(6): 775–780.

[12] Hoang, T.; Choi, D.; and Nguyen, T. (2015), Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *Int. J. Inf. Sec. Springer*. DOI 10.1007/s10207-015-0273-1

[13] Wong (1998), A Watermark for Image Integrity and Ownership Verification. *IS&T's 1998 PICS Conference Copyright*: 374-379.

[14] Miguel A. Ferrer, Moisés Díaz, Aythami Morales , "Synthetic Off-line Signature Image Generation", in Proceedings of 6th IAPR International Conference on Biometrics, Madrid, Spain, 4-6 June 2013.3.5.

[15] Lee, Y.P., Lee, J. C., Chen, W.K. (2012), Chang, K.C., Su, I.J., and Chang, C.P., High-payload image hiding with quality recovery using tri-way pixel-value differencing. *Information. Science.* Vol, 191: 214–225.

[16] Bhatnagar, S., Kumar, S, and Gupta, A. (2014), An Approach of Efficient And Resistive Digital Watermarking using SVD. *IEEE, 2014 International Conference on Advances in Computing,Communications and Informatics (ICACCI),Jaypee University of Engineering and Technology, Guna, India* :2470– 2475.

Jyotika Chopra did her Bachelor of Engineering in Electronics and Communication Engineering from Bhai Gurdas Institute of Engg & in 2006. She did her Master of Technology from Dr. B. R. Ambedkar National Institute of Technology (NIT) Jalandhar in 2008.She worked on the post of lecturer in Lovely Professional University Phagwara , as Assistant Professor in RIMT Mandi Gobindgarh and CGC Landran. She is also pursuing her Ph.D from Sant Longowal of Engineering.

Amod Kumar is currently working as Chief Scientist in Central Scientific Instruments Organisation, Chandigarh. He did his Ph. D. from IIT Delhi in 2005, M. E. in Electronics from Punjab University, Chandigarh in 1985 and B. E. (Hons.) from Birla Institute of Technology and Science, Pilani (Raj.) in Electrical and Electronics Engineering in 1979. He has more than 37 years' experience in R & D in the areas of process control, environment monitoring, biomedical engineering and prosthetics. His areas of interest are embedded systems, digital signal processing and Soft Computing.

Anupma Marwaha is working as Professor and Head of Department of Electronics & Communications in Electronics and Communication Engineering Department at SLIET Longowal, Sangrur. She did BE in Electronics and Communication Engineering from PEC Chandigarh in 1990 & M. Tech from REC Kurukshetra in 1992. She completed Ph. D. in Electronics from GNDU, Amritsar in 2003.She is a fellow member of ISTE, New Delhi and Institution of Engineers, India .Her continuing research interests primarily underpin the overarching notion that there are many underutilized, yet powerful ways in which electromagnetic phenomena may be exploited in the area of bio-medical engineering and in microscale and nanoscale structures at large.

Sanjay Marwaha born on April 1966 at Nahan. Dr. Marwaha is Professor and Head in the Department of Electrical and Instrumentation Engineering at SLIET, Longowal. He did his BE (Electrical Engg.) from Gorakhpur University, Gorakhpur in 1988, ME (Power Systems) from Punjab University, Chandigarh in 1990 and Ph.D. from GNDU, Amritsar in 2000. He is life member of ISTE and Member, Institution of Engineers (India) and has published around 160 research papers in National and International journals/conferences of repute. He has been conferred 3 awards by different organizations for his academic excellence. His area of interest includes Design and Analysis of Electromagnetic Devices, Power Systems and HV Engg. Electrical and Electronic Measurements and Instrumentations, Industrial Electronics and Microwave Engineering.