MITIGATING IRIS BASED REPLAY ATTACK USING CUCKOO OPTIMIZED REVERSIBLE WATERMARKING

Richa Gupta* and Priti Sehgal**

* **University of Delhi
richie.akka@gmail.com, psehgal25.08@gmail.com

ABSTRACT: Replay attack on biometric pose a challenge to the security of biometric recognition systems. Many researchers have proposed the algorithms for watermarking the biometric data to mitigate replay attacks but most of them usually compromise with the recognition performance of biometrics. In this paper, an algorithm that selects an optimal bit plane using cuckoo based optimization is proposed, to hide the watermark in iris biometric using reversible integer wavelet transform. The algorithm minimizes the compression ratio of image, leading to invisible watermarking. The use of reversible watermarking has an advantage of retrieving the original biometric back from the watermarked image without any loss of precision and impact on recognition performance. The proposed algorithm uses the sensor ID combined with current date and time as watermark. This choice of watermark propels the verification at the extraction end and hence detects whether it is replayed data or the fresh sample. The recognition performance of iris before and after watermarking has also been compared and the results are found to be same.

KEYWORDS: Biometrics, watermarking, optimization, IWT, replay attack.

INTRODUCTION

Biometric enables the unique identification of a person. The limitations in traditional security of the system is paving a path for biometric based recognition. Amongst several biometrics like fingerprint, voice, gait etc. iris is considered to be most accurate. The easiness to capture the iris sample and yet its accuracy makes it a crucial biometric for authentication. Security of iris biometric is of prime concern as its compromise can lead to breach of security in highly critical areas of its application. Iris is widely studied under various attacks such as template attack and print attack. Another attack, known as replay attack has been one of the common problem faced during iris biometric authentication. Replay attack comprises of illegal interception of data over network and its re-submission to the system. Hence an intruder pretends himself to be an authentic user, in order to enter the system. Replay attacks pose a hazard to the integrity of system. Interception of data over network can not only permanently reveal the biometric identity of the user but also make that biometric unusable for future use. Security of iris biometric has been widely studied by researchers in the area of stored template attack and its liveness detection at the sensor. Very little research has been carried out with respect to replay attacks [1], [2], [3].

Digital watermarking is hiding some unique identity in the data while transmitting it over the network. The two basic characteristics for digital watermarking are: 1) Watermark should be imperceptible to the viewer, that is, the embedding process should not deteriorate the quality of the watermarked image. 2) Watermark should be robust, that is, one should be able to extract the watermark after certain distortions in the image. Digital watermarking although provides protection, is lossy. The original data cannot be extracted back from the watermarked content and hence there is significant loss of precision. Reversible watermarking in this context is of high usage. It allows to obtain the exact replica of original content from the watermarked image. Reversible watermarking can be categorized into fragile and semi-fragile reversible watermarking. In fragile reversible watermarking, the watermarked image is very sensitive to modifications and it tends to lose the inserted watermark even on slight modification (like JPEG compression, noise) in the image. Thus, revealing the fact that the data has been modified. In semi-fragile reversible watermarking, watermarked image is able to survive unintentional attacks like slight JPEG compression attack [4].

The watermarking algorithms have been proposed to mitigate several attacks. Some of them have been further discussed here. J.Dong [5] studied the effect of watermarking on iris biometric under two scenarios: protecting iris images (i.e. using it as cover image) and using iris as watermark. They reported that not much of a significant decrease occurs in the performance of iris recognition algorithm. But, watermarking attacks in certain cases can degrade the performance. N.Bartlow [6] studied the result of watermarking voice descriptors on iris image and found negligible impact on matching performance. In other approach, M.Fouad [7] proposed a technique for iris template protection. They shuffle the iriscodes and use it as watermark to be embedded in a cover image. The shuffling ensures that a new template could be generated in case database is compromised. They found that attacks on watermarked image do degrade the performance of recognition system to a certain extent. J.Hammerle [2] also made an experimental study on 10 watermarking algorithms. They used sensor ID as watermark embedded in captured iris image (cover image). They found that some of these approaches severely degrade the iris recognition performance. The use of reversible watermarking can relieve from performance degradation.

In this paper, a method of finding the best bit plane to hide the watermark in wavelet domain using reversible integer wavelet transform with cuckoo based optimization has been proposed. The algorithm results in low compression ratio and high imperceptibility. The reversible nature of algorithm enables it to extract the original biometric from the watermarked image. Its fragile property makes it highly susceptible to slightest modification. Thus, it can be detected that the data has been modified and is not suitable for authentication. This method of watermarking can help to mitigate replay attack by verifying the originality of data received. In section 2 and 3, reversible integer wavelet transform based watermarking and cuckoo based optimization respectively, have been further discussed.

REVERSIBLE INTEGER WAVELET TRANSFORM BASED WATERMARKING

Watermarking is an important step in digital era to secure the originality of the data. But, there are certain cases, where just recovering the owner's information of host data is not important, recovering the original un-watermarked content is also necessary. For instance, it is important to avoid any compromise with the accuracy of iris recognition system. This has promoted the idea of reversible watermarking and several techniques for reversible watermarking can be seen in literature [8]. In this paper, we propose to use wavelet domain based integer wavelet transform (IWT) for watermarking the iris images. Unlike discrete wavelet transform (DWT), IWT transforms the image into another set of integer data, thus allowing the perfect reconstruction of the original data [9], [8]. IWT based reversible watermarking is fragile in nature and is prone to slightest modification. In this paper, Cohen-Daubechies-Feauveau wavelets (cdf2.2) have been used to change the image to wavelet domain. The transform coefficients obtained are integers and hence no truncation is required, which is the main reason for these techniques being irreversible.

CUCKOO BASED OPTIMIZATION

The nature inspired “cuckoo optimization algorithm” was first presented by [10]. This algorithm found its inspiration from a bird named Cuckoo, whose nature is laying his own eggs in other birds’ nests. It starts by laying down the eggs in a nest which is chosen randomly, similar to other nature inspired optimization algorithms. The best survival rate of a nest forms the basis of Cuckoo Optimization Algorithm. The eggs are discovered by the host bird with probability pa Є (0,1). To generate new solutions x(t+1) for ith cuckoo, Levy flights is used as given by equations (1) and (2) [11], [12].

$$x_i^{(t+1)} = x_i^{(t)} + \alpha \oplus Lévy(\lambda) \tag{1}$$

where, $\alpha > 0$ is the step size which controls the scale of random search.

The Levy flight enables random walk whereas random step is drawn from a Levy distribution as follows:

$$Lévy \sim u = t^{-\lambda}, \quad (1 < \lambda \leq 3) \tag{2}$$

Cuckoo algorithm has been used by many researchers as an optimization tool and its results are juxtaposed with several already existing optimization techniques. J.Waleed [12] proposed the selection of optimal positions to hide the watermark in the cover image using cuckoo optimization. The results are compared to other nature inspired algorithms such as Particle Swarm Optimization (PSO) and Bee Algorithm (BE), which shows that cuckoo optimization performs quite better in terms of performance when comparing PSNR and Normalized Correlation Coefficient (NC) values. M.Ali [13] proposed the technique of optimizing the scaling factor for watermark image. The scaling factor is crucial to determine the imperceptibility and robustness of watermark in an image. They tested their approach after various attacks and found that optimally selecting the scaling factor using Cuckoo based optimization results in better PSNR values as compared to using no optimization at all. Also, the approach was found to be robust against several watermarking attacks (like gamma correction, cropping etc.). A.Singhal [14] proposed the use of cuckoo algorithm to optimally find best coefficients in discrete wavelet transform of an image to embed secret data for transmission. They compared their

result with PSO based watermarking approach proposed by R.Bansal [15] and found results to be better in terms of PSNR and SSIM values. Cuckoo search algorithm has been widely deployed in many application as in multi-objective optimization [18], segmentation of retinal images [19].
Here, we have used the simplest solution where each egg corresponds to one nest and each cuckoo can lay one egg, i.e., it represents one solution [11], [16], [10], [17]. The fitness value (explained in section 3.1) is calculated for each nest (that is, each bit plane) and best nest is selected.

Fitness Function for Cuckoo Based Optimization

Image Compression has been used as the fitness function in this paper. The compression can be reversible and irreversible. The reversible compression helps in regenerating the authentic image from the compressed image without any deformation. The irreversible compression does not preserve the original image exactly, leading to certain distortions. Minimizing the compression ratio helps to determine if the compressed part of an image has sufficient bandwidth to accommodate the watermark. It also helps to maximize the PSNR ratio of an image, and hence increasing the imperceptibility of the watermark in the image. Image compression is of wide importance in medical images [20], [21], [22]. It aims at saves the bandwidth without any significant loss of information. This paper optimizes the compression ratio of an image which is the given as

$$CompressionRatio(CR) = \frac{uncompressed \text{ or } original\ image \text{ size}}{compressed\ image \text{ size}} \quad (3)$$

The compression ratio for each bit plane is used as fitness function for cuckoo's algorithm. It is minimized and optimal bit plane is selected to hide the watermark.

PROPOSED FRAMEWORK

To allay the problem of forged identification with respect to replay attack, we present the use of reversible integer wavelet transform based watermarking. The watermark in our approach comprises of a unique sensor ID, current date and time. This helps the system, at the time of authentication, to identify whether the presented biometric sample belongs to the user or is a stale version of his biometric captured and is presented illegally.
The watermark is hidden in LH, HL and HH (vertical, horizontal and diagonal) sub-band of integer wavelet transform as these bands contain the finer details of the image and thus hide the data without much perceptible changes to the viewer. Every time, a sub-band is selected and is given to cuckoo optimization algorithm. The nest with best survival rate, that is, one with minimum fitness value is selected and is taken to the next iteration. The system decomposes the LL sub-band further and each sub-band is given to cuckoo optimization algorithm. This process is continued till no further improvement is seen. This selects the optimally chosen bit plane with minimum compression ratio and thus increase the imperceptibility of watermark hidden.
Watermark is embedded in the selected bit plane by first compressing the LH, HL and HH sub-bands using arithmetic coding, and appending the watermark to it. This extended string is then embedded to the iris (cover) image [23] and inverse IWT transform is applied to obtain the watermarked image. The algorithms for embedding and extraction of watermark has been illustrated in Figure 1 and 2 respectively.

EXPERIMENTAL RESULTS

Experiments were conducted on Casia-Iris-Interval database[1] developed by Chinese Academy of Sciences (CAS) to promote the academic research. It consists of images from left and right iris from 249 subjects, consisting of a total of 2639 grayscale iris images. All images are 320x280 pixels, which are presented to Iris OSIRIS version 4.1[2] and normalized images are obtained. These are taken as host images. Some of the sample images used for watermarking are shown in Figure 3. The watermark to be embedded is a string consisting of sensor ID, current date and time. This will help system to identify the replay attack. If the time extracted from watermark is beyond the threshold set by the system administrator, it can be rejected.
Experimental results reveal, as shown in Figure 4 and 5, that PSNR[3] and SSIM [14] values, as defined by equation (4) and (6) respectively, for proposed approach are clearly better than fixing a bit plane for embedding the watermark.

[1] http://www.csse.uwa.edu.au/~pk/studentprojects/libor/sourcecode.html
[2] http://svnext.it-sudparis.eu/svnview2-eph/ref_syst/Iris_Osiris/
[3] http://in.mathworks.com/help/vision/ref/psnr.html

Embedding

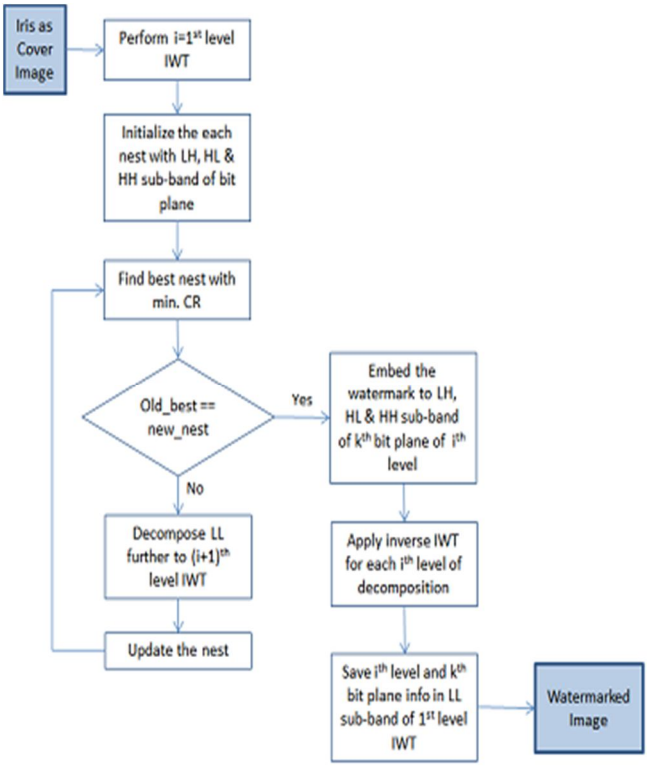

Fig. 1. Embedding Algorithm

Extraction

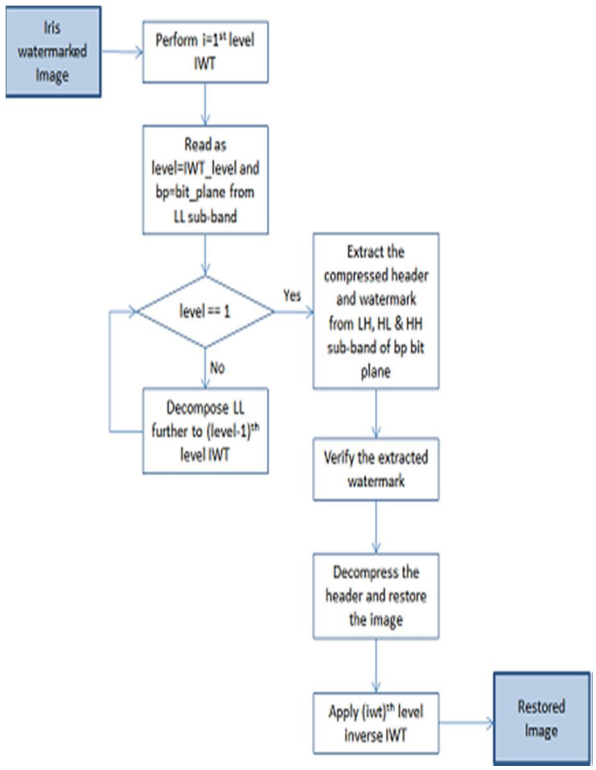

Fig. 2. Extraction Algorithm

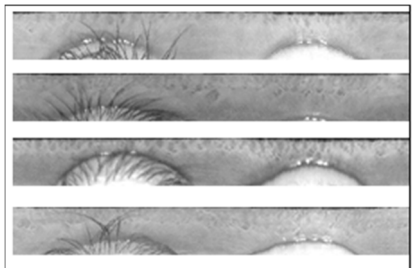

Fig. 3. Sample host images for randomly chosen iris

$$PSNR = 10log\left(\frac{X^2}{MSE}\right) \quad (4)$$

$$MSE = \frac{\sum_{R,C}[O(r,c)-W(r.c)]^2}{R*C} \quad (5)$$

where,
X is the maximum value in the watermarked image
O and W is original and watermarked image respectively
R, C are rows and columns in input image respectively

$$SSIM = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_1)}{(\mu_x^2+\mu_y^2+C_2)(\sigma_x^2+\sigma_y^2+C_2)} \quad (6)$$

where,
μ_x: average of x
μ_y: average of y;

σ_x^2: variance of x;
σ_y^2: variance of y;
σ_{xy}: covariance of x and y;
L: dynamic range of pixel values
$k_1 = 0.01, k_2 = 0.03$ default values
$C_1 = (k_1 L^2), C_2 = (k_2 L^2)$ variables to stabilize weak denominator

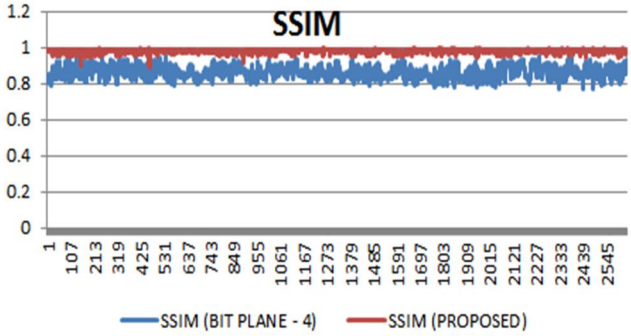

Fig. 4. Comparative result of SSIM values for IWT (with fixed bit plane 4 as suggested by [23]) and proposed (with Cuckoo Optimization)

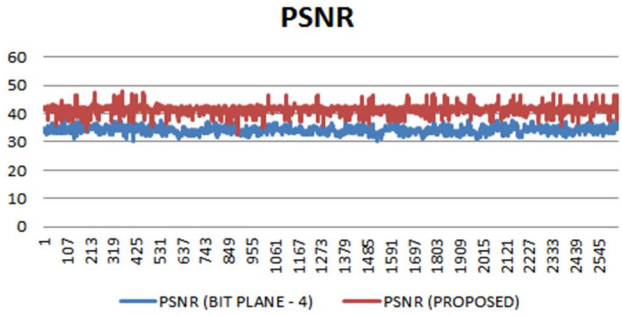

Fig. 5. Comparative result of PSNR values for IWT (with fixed bit plane 4 as suggested by [23]) and proposed (with Cuckoo Optimization)

The matching performance of iris using Iris OSIRIS version 4.1 has also been compared. For this, from each set of images per subject per eye, the first image is taken as test image and rest of the images are considered as reference images. The normalized iris images are replaced with iris images restored after extracting the watermark and matching results of the two scenarios are compared. The results reveal that there is no difference in the hamming distance of two scenarios, thus achieving the whole idea of using reversible watermarking in wavelet domain.

CONCLUSION

The cuckoo inspired optimization on IWT based reversible watermarking is discussed in this paper. This selects the optimal bit plane to hide the watermark which optimizes the compression ratio. The extracted watermark can be compared with the original watermark to verify the iris biometric against replay attack. If sensor ID matches in both the watermarks and date-time is within the permissible limit, considering the transmission time, biometric is considered to be an authentic copy. Otherwise, it is discarded. This helps to mitigate the replay attack on biometric. Experimental results were verified on Casia-Iris-Interval DB on 2639 images to compare the PSNR ratio and SSIM similarity index. The recognition performance on iris is also compared using Iris OSIRIS v4.1.
Replay attack mitigation using DWT based watermarking and cuckoo's optimization results in better PSNR values. But, this has a limitation, as stated above, it is not reversible which is important to ensure performance of iris recognition system. This can be successfully achieved by using reversible watermarking with cuckoo based optimization approach.

FUTURE WORK

This work can further be extended by using some cryptographic technique to generate a key. This key can be used to map the locations selected by the proposed approach and provide another level of security. The cryptographic key based on biometric of a person would provide two-fold security.

REFERENCES

[1] Czajka, A., Pacut, A.: Replay attack prevention for iris biometrics. In: 2008 42nd Annual IEEE International Carnahan Conference on Security Technology. pp. 247–253. IEEE (2008).

[2] Hämmerle-Uhl, J., Raab, K., Uhl, A.: Robust watermarking in iris recognition: Application Scenarios and Impact on Recognition Performance. ACM SIGAPP Applied Computing Review. 11, 6–18 (2011).

[3] Shelton, J., Roy, K., O'Connor, B., Dozier, G. V.: Mitigating Iris-Based Replay Attacks. International Journal of Machine Learning and Computing. 4, 204–209 (2014).

[4] Caldelli, R., Filippini, F., Becarelli, R.: Reversible watermarking techniques: An overview and a classification. Eurasip Journal on Information Security. 2010, (2010).

[5] Dong, J., Tan, T.: Effects of watermarking on iris recognition performance. 2008 10th International Conference on Control, Automation, Robotics and Vision, ICARCV 2008. 1156–1161 (2008).

[6] Bartlow, N., Kalka, N., Cukic, B., Ross, A.: Protecting Iris images through asymmetric digital watermarking. 2007 IEEE Workshop on Automatic Identification Advanced Technologies - Proceedings. 192–197 (2007).

[7] Fouad, M., Petriu, E.: Combining DWT and LSB watermarking to secure revocable iris templates. 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA), IEEE. 25–28 (2010).

[8] Narawade, N., Kanphade, R.: Reversible Watermarking: A Complete Review. International Journal of Computer Sciences and Telecommunications. 2, 1–5 (2011).

[9] S Jayasudha: Integer Wavelet Transform Based Steganographic Method Using Opa Algorithm. International Journal of Engineering and Science. 2, 31–35 (2013).

[10] Yang, X.S., Deb, S.: Cuckoo search via Levy flights. 2009 World Congress on Nature and Biologically Inspired Computing, NABIC 2009 - Proceedings, IEEE. 210–214 (2009).

[11] Yang, X.-S.: Nature-inspired metaheuristic algorithms. Luviner Press (2010).

[12] Waleed, J., Jun, H.D., Hameed, S., Kamil, M.: Optimal Positions Selection for Watermark Inclusion based on a Nature Inspired Algorithm. International Journal of Signal Processing, Image Processing and Pattern Recognition. 8, 147–160 (2015).

[13] Ali, M., Wook, C.: An optimal image watermarking approach through cuckoo search algorithm in wavelet domain. International Journal of System Assurance Engineering and Management. 1–10 (2014).

[14] Singhal, Anuradha and Bedi, P.: Steganography using Cuckoo Optimized Wavelet Coefficients. Proceedings of the Third International Symposium on Women in Computing and Informatics. ACM. (2015).

[15] Bansal, R., Sehgal, P., Bedi, P.: Securing Fingerprint Images Using PSO-Based Wavelet Domain Watermarking. Information Security Journal: A Global Perspective. 21, 88–101 (2012).

[16] Waleed, J., Jun, H. D., Abbas, T., Hameed, S., & Hatem, H.: A Survey of Digital Image Watermarking Optimization based on Nature Inspired Algorithms NIAs. International Journal of Security and Its Applications. 8, 315–334 (2014).

[17] Yang, X. S., & Deb, S.: Engineering optimisation by cuckoo search. International Journal of Mathematical Modelling and Numerical Optimisation. 1, 330–343 (2010).

[18] Yang, X.S., Deb, S.: Multiobjective cuckoo search for design optimization. Computers and Operations Research. 40, 1616–1624 (2013).

[19] Srishti: Technique based on Cuckoo ' s Search Algorithm for Exudates Detection in Diabetic Retinopathy. Student, M., Electrical Engg Deptt, and Deenbandhu Chhotu Ram.

[20] Rani, J., Khan, T.A.: Performance Optimized DCT Domain Watermarking Technique with JPEG. International Journal of Innovative Technology and Exploring Engineering (IJITEE). 20–24 (2014).

[21] Badshah, G., Liew, S., Zain, J.M., Hisham, S.I., Zehra, A.: Importance of Watermark Lossless Compression in Digital Medical Image Watermarking. Research Journal of Recent Sciences. 4, 75–79 (2015).

[22] Veera Swamy, K., B., C.M., Y.V, B.R., S., S.K.: Image Compression and Watermarking scheme using Scalar Quantization. International Journal of Next-Generation Networks. 2, 37–47 (2010).

[23] Xuan, G., Zhu, J., Chen, J., Shi, Y. Q., Ni, Z., & Su, W.: Distortionless data hiding based on integer wavelet transform. Electronics Letters, IEEE. 38, 1646–1648 (2002).