Iris Biometric Watermarking for Authentication Using Multiband Discrete Wavelet Transform and Singular-Value Decomposition

Original Scientific Paper

S. Joyce
Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, India.
joyceimmanuel13@gmail.com

S. Veni
Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, India
venikarthik04@gmail.com

Abstract *– The most advanced technology, watermarking enables intruders to access the database. Various techniques have been developed for information security. Watermarks and histories are linked to many biometric techniques such as fingerprints, palm positions, gait, iris and speech are recommended. Digital watermarking is the utmost successful approaches among the methods available. In this paper the multiband wavelet transforms and singular value decomposition are discussed to establish a watermarking strategy rather than biometric information. The use of biometrics instead of conservative watermarks can enhance information protection. The biometric technology being used is iris. The iris template can be viewed as a watermark, while an iris mode of communication may be used to help information security with the addition of a watermark to the image of the iris. The research involves verifying authentication against different attacks such as no attacks, Jpeg Compression, Gaussian, Median Filtering and Blurring. The Algorithm increases durability and resilience when exposed to geometric and frequency attacks. Finally, the proposed framework can be applied not only to the assessment of iris biometrics, but also to other areas where privacy is critical.*

Keywords*: Biometric Watermarking, Multiband Discrete Wavelet Transform, Information Security, Frequency Domain Watermarking*

1. INTRODUCTION

In the second half of the 20th century, the World Wide Web or WWW phenomenon, demonstrated the economic value of offering digital media free of charge. The use of digital networks to include digital media for commercial purposes is expected of multinationals (MNCs) [1]. But also, their ownership must be protected. It is thus a popular encryption method that is using encryption and other alternative methods (digital watermarking). Because of using advanced tools for copying and modifying multimedia data, safety becomes a major problem. Digital multimedia data are therefore very critical to preserve. Digital information, like digital pictures, audial and audio-visual, is widely available. Might not display the watermark. For photographs and videos, Visible watermarks are used, but they typically ruin elegance, whereby the location of the imprint is exposed to the attacker. It ran to an invisible watermark's popularity, when the watermark's position is not public. In the space or transformation field, the invisible watermarking can be performed.

The presented approach is a variant range due to the additional robustness of the same function [2].

Watermarking can be applied using a number of techniques in the transform domain, including the Fourier Transform, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and others. A hybrid conversion domain based on DWT and SVD is used in this example. This is because DWT's multi-resolution function enhances recognizability, while SVD improves the system's robustness [3,4]. Unlike the conventional method, which uses an image or signal as a watermark, the user's iris biometric information is used as a watermark in this method. In this case user ID is used, like how a logo can be used as a watermark in different ways. The security level has improved many times since biometric technology is based on the principle of "what are you," as opposed to the conventional watermarking approach [5].

The Iris biometric watermarking enhances the security of the system by using the Fourier Transform technique. The encryption is processed along with the biometric watermarking. The watermarking technology is used to protect the biometric data. Mainly the proposed method focuses on increasing the security of the iris biometric using watermarks from the host rather than the authentication from the client side. Fig1 shows

The working of the Iris Recognition System and the Feature Extraction using Fast Wavelet Transform an Iris image is segmented, normalized, Feature Extraction is done with binary signature, comparison is done and the Iris is stored in the Template.

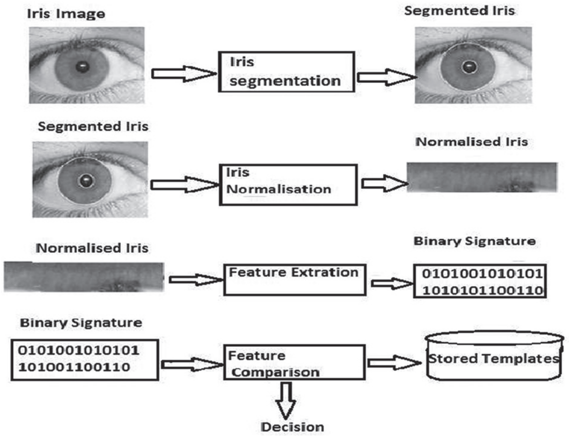


Fig. 1. Working Flow of Iris Recognition System

1.1. ADVANTAGES OF BIOMETRIC WATERMARKING

Jain et al. [19] suggested watermarking technology, as a second protective action for biometric systems. The use of watermarking will increase the safety and reliability of the biometric system efficiently [7]. Biometric watermarking benefits are listed:

The watermark is invisibly hidden in host data and can be used as an authentication token for security purposes. When biometric data are intercepted, a tracking system may be established to identify the data source.

- The host data has been connected to the watermarked information so that there is no further storage or transfer of resources needed. Furthermore, 'on-site' authentication doesn't require biometric or watermark database privileges.
- Other protection tools will not be affected by watermark. Cryptographic operations or template security methods may either be used with watermarked data or with watermarked host data.

1.2. WATERMARKING AND IRIS BIOMETRIC TECHNOLOGY

Two approaches are taken to incorporate biometric technology and watermarking technology. First, watermarking biometric data is used to protect biometric data privacy and to improve safety as a watermarking host [8]. The second is the biometric watermark used for authenticating the host image. The second form of role here is [9]. Researchers used the second watermark security system primarily with fingerprints and facets on biometric host images in the past [10,11].

2. RELATED WORKS

Watermarking technology is used to hide information in the host data image in order to protect its integrity. For embedding data into photographs, there are many watermarking techniques. They are known as spatial domain technologies [12, 13] and frequency domain technologies [14, 15, 16, 17]. While possessing the lowest complexity and maximum load power, space technology is vulnerable to occurrences such as image manipulation and low-pass filtering [18].

The spatial domain technologies include the mathematical processing of image pixel data to emphasize spatial relationships and the process again defines the homogeneous regions based on linear edges.

The frequency domain is the space defined by Fourier transform. Frequency domain analysis is used to indicate how the signal energy can be distributed in the range of frequency.

A watermark-based approach is proposed in [19, 20] in which the biometric system is safe and immune to cautious manipulation and attacks. Here it remains no research has been done into the integrity and robustness of biometric data under multiple attacks. A new biometric watermarking algorithm is developed in this white paper to reduce the vulnerability of biometric systems to geometric and frequency attacks. The mixture of wavelet and LSB-based watermarking technology, a watermark fingerprint is produced by inserting a prototype or facial image into the fingerprint image. Watermarking technology based on wavelets can withstand frequency attacks which is vulnerable to geometric outbreaks. LSB-based watermarking procedures, on the other hand, can withstand geometric attacks but are vulnerable to frequent outbreaks.

Low et al. [21] to decompose the signature into a string of binary bits, use the Discrete Random Transform (DRT) and Principal Component Analysis (PCA). The three implanting and removal approaches are compared to assess the robustness and power of JPEG compression. They are Least Significant Bit (LSB) and Code Division Multiple Access (CDMA) spread range in the spatial domain, and also in DWT domain. Humanoid visual observation, Peak Signal-to-Noise Ratio (PSNR), and alteration factor are used to determine the output of these approaches (standardized Hamming distance). The results show that, regardless of having the easiest contact to biometric watermarks, the LSB process is extremely susceptible to JPEG compression. The CDMA spread range in the DWT area is complex, but it is further hard for JPEG compression.

By combining encryption and watermarking techniques, Fouad et al. [22] identified a method for protecting iris patterns. A key protects the iris file, which is inserted in the original image using LSB and DWT technology. The second key specifies the containment location. Two keys are required for iris extraction (iris and embedded).

Majumder et al. [23] apply biometric watermarking the Discrete Wavelet Transform (DWT) method, SVD (singular value decomposition) of the host copies to obtain the eigenvectors. Using Discrete Cosine Transform (DCT) technology, extract iris features and include them in the function vector. The downside of this approach is that you cannot modify the procedure for iris feature extraction.

Paunwala and Patnaik [24] inserted fingerprint and iris structures, block-divided cover image. Convert each block to a two-dimensional DCT and mark it as having or not having edges. In the low-frequency coefficient 8 x 8 DCT block, the edge block is omitted because the biometric recognition feature is built.

To improve protection, Lu et al. [25] planned a method that relies on iris recognition somewhat than digital watermarking. For error control, DCT is applied to the iris pattern, and the resulting rate is encoded using the Bose-Chaudhuri-Hocquenghem (BCH) code. The host image is split down into four similar blocks. In BCH code, the particular value is inserted in each coefficient in the host image using the key attained by the DCT procedure. The inverse cosine transforms (IDCT) are used in the image after adjusting the DCT coefficients of the host image in the watermark. Here the watermark's intensity is determined by the key used. The results show that this process is capable for extracting the watermark.

3. PROPOSED BIOMETRIC WATERMARKING ALGORITHM

The iris copy is used as the base or cover image for watermarking, a regular logo is used as the watermark. Iris characteristics are obtained through the process of iris localization and standardisation. It is classified into two parts: watermark implanting and watermark removal.

3.1 PREREQUISITES OF WATERMARK ALGORITHM

The following are the steps involved in the pre-processing steps for the cover image and watermark.

In Dual Tree Wavelet Transform, a time-frequency investigation method is used. Wavelet Transform allows for multi-resolution attribute study. In the four sub images with each point, equal sizes will be detected. LL_k will be chosen as estimated sub images, with LH_k, HL_k, and HH_k referring to horizontal, vertical, and diagonal direction greater-frequency aspect sub images.

The $k = 1,2,3,...(k \in N)$ will be referred to as the scale or status of the wavelet breakdown.

In the distribution of parallel spatial localization and frequency distribution relating to the watermark within the host image, the Multiband Dual Tree Discrete Wavelet Transform will be heavily used. The fundamental principle existed with the use of Multiband Dual Tree Discrete Wavelet Transform for image processing would be with many distinct halts of the image into sub images comprising diverse spatial domains and autonomous frequencies.

The data may be twisted within the calculation of the arrangement for implanting the watermarking procedure inside the element, which may be involved in debasing the intensity of the created watermark. Estimate, sub-image coefficients are chosen for imbedding watermark to ensure the provision of an invisible watermark as well as better power. Fig. 2. shows the conversion of an isolated wavelet has been completed.

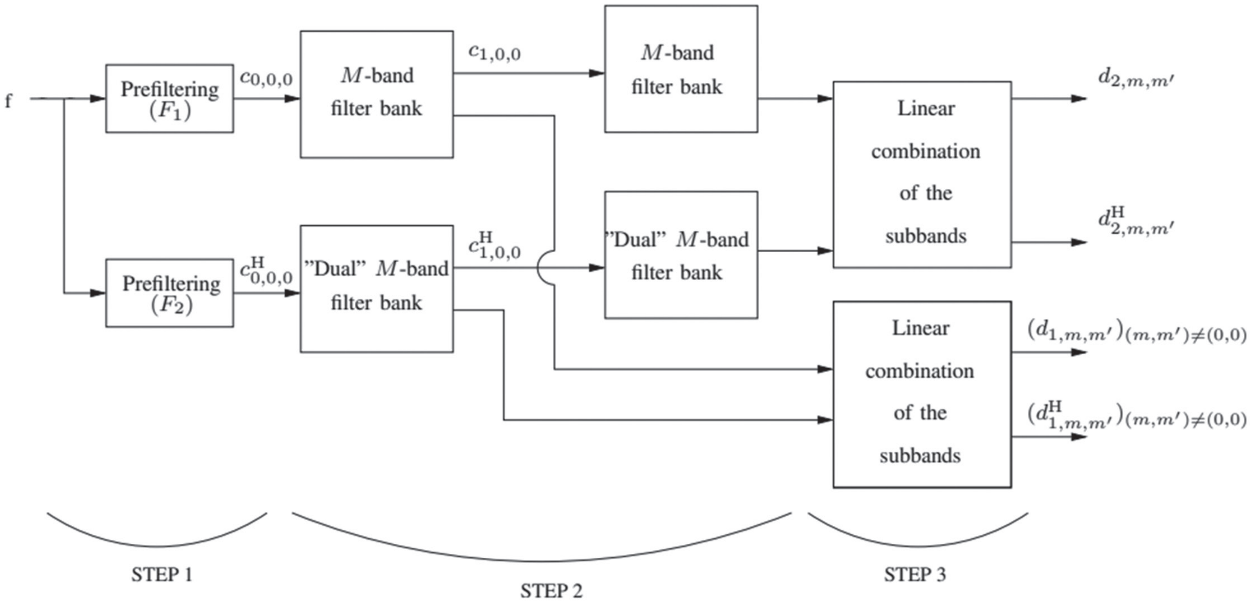

f
Prefiltering (F_1)
$c_{0,0,0}$
M-band filter bank
$c_{1,0,0}$
M-band filter bank
Linear combination of the subbands
$d_{2,m,m'}$
$d^{H}_{2,m,m'}$
Prefiltering (F_2)
$c^{H}_{0,0,0}$
"Dual" M-band filter bank
$c^{H}_{1,0,0}$
"Dual" M-band filter bank
Linear combination of the subbands
$(d_{1,m,m'})_{(m,m')\neq(0,0)}$
$(d^{H}_{1,m,m'})_{(m,m')\neq(0,0)}$
STEP 1
STEP 2
STEP 3

Fig. 2. M-band Dual-Tree Decomposition Scheme Over 2 Resolution Level

1) Singular Value Decomposition (SVD)

The process of Singular Value Decomposition (SVD) involves breaking down a matrix A into the form. This computation allows us to retain the important singular values that the image requires while also releasing the values that are not as necessary in retaining the quality of the image.

The original matrix A will be designated as an image with a size of $m*n$, and the breach down of A will be provided in the following expression:

$$A= U\,S\,V^{T} \tag{1}$$

Singular Value Decomposition of A will be the breakdown process, as U is a unitary matrix of dimension $m*m$, S is a matrix of positive numbers to the diagonal and Zeros found in positions other than the diagonal of dimension $*n$, and the conjugate transpose of VT, is unitary of measurement $n*n$. The luminance of the image will be represented by positive values of matrix S. Changing positive S ideals would not affect image excellence. They cannot be changed, either, even if there's an intruding impact. Watermarking techniques took advantage of these characteristics.

2) Arnold Transform

Arnold transform is widely used in image stenography, authentication, and tamper detection, self-recovery and image cryptography algorithms. In all these cases, Arnold transform is used as a scrambling step in which the number of iterations is used as a key.

Arnold Transform can perform arbitrary positioning of individual picture elements in relation to the original image. However, if the process is repeated for enough times, it is found the unchanged image reappears. In Arnold Transform, a change in position from one point to the next can be found. The Arnold transformation will be used to convert a digital image with dimension $N*N$.

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} mod(n) \tag{2}$$

While $i, j \in \{0, 1,...., N\text{-}1\}$, while (i, j) are the coordinates that define the location of pixels in the actual image. (i', j') will coordinate that describe the location of pixels after the entire coordinates have been transformed, resulting in a disoriented image.

3.2. PROPOSED WATERMARKING ALGORITHM USING MULTIBAND DTDWT

The initial generation of the Watermark image will take into account for the iris image, and then the image will be transformed into one that only contains binary values. Following that, the Iris image will go through a 3-Stage Wavelet breakdown with 2D Coefficients. The watermark will be implanted after the Approximation sub-band LL3 has been selected. Prior to the implanting process, the created watermark will be converted to Arnold format. Following that, watermarked coefficients will be created by applying the SVD transform to the watermarked image along with the sub-band of choice. Following that, the watermarked image with the implanted watermark will be generated using the inverse Discrete Wavelet Transform. The procedure for extracting the watermark would be reversed from the procedure used to implant it.

Fig. 3 depicts the proposed algorithm's step-by-step movement. The iris image will be used as the concealed image, while the binary image will be used as the watermark. The proposed procedure is separated into two sections: 1. Embedding and 2. Extraction.

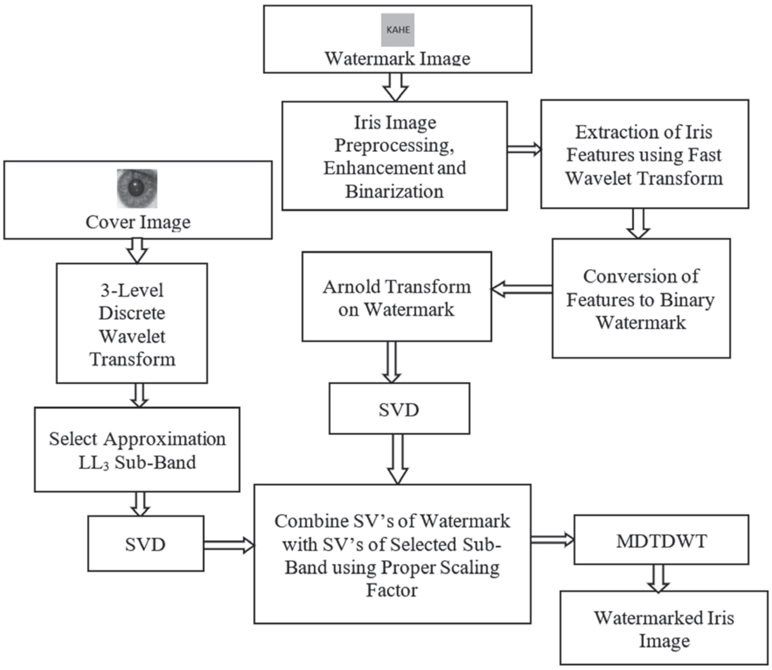

KAHE
Watermark Image
Iris Image Preprocessing, Enhancement and Binarization
Extraction of Iris Features using Fast Wavelet Transform
Cover Image
3-Level Discrete Wavelet Transform
Arnold Transform on Watermark
Conversion of Features to Binary Watermark
SVD
Select Approximation LL₃ Sub-Band
SVD
Combine SV's of Watermark with SV's of Selected Sub-Band using Proper Scaling Factor
MDTDWT
Watermarked Iris Image

Fig. 3. Watermark Implanting Model

3.2.1. Watermark Embedding Scheme

The following are the steps involved in embedding the Watermarks into the host image:

Step 1: Multiband DTDWT is used to break down an iris image. The LL3 approximation sub-band will be chosen from all of the obtained sub-bands.

Step 2: Pre-analysis of Iris Image Breaks in the Iris Image will be observed, and fake points will be produced. The mining would subsequently be performed by standardisation and frequency assessment. The use of measured frequencies will be defined for filtering using Gabor Wavelet.

Step 3: The Multiband Wavelet Transformation is the abstraction of iris features and the replacement of features of iris images.

Step 4: Convert the Watermarked Image $_W$ using Arnold Transform.

Step 5: The Watermarked Coefficients A_W is achieved by accepting below three stages:

1. $A= U S V^T$

2. $S +\alpha_W = U_W S_W V_W^T$ While α is a watermark asset

3. $A_W = US_W V^T$

Step 6: Reverse wavelets are used to modify the picture from a true double precision to an unsigned 8 bit integer. The picture of a watermark is created in relation to the implantation of a watermark.

Step 7: The procedure for embedding watermark is completed.

3.2.2. Watermark Extraction Scheme:

The watermarking can be extracted by executing the opposite order of watermark imbedding procedure.

Step 1: The low-frequency wavelet coefficient LL_3 is selected to perform a multiband dual tree wavelet transform on a watermarked image.

Step 2: Implement Singular Value Decomposition (SVD) with respect to A^*, the instruction is obtained as $A^* =U^* S_1^* V^{T*}$, along with accomplish U^*, S_1^* and V^{T*}.

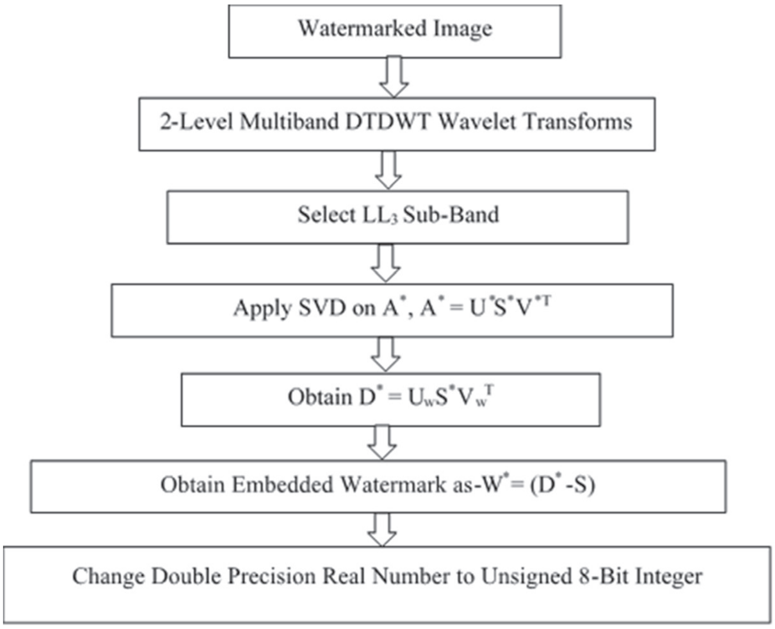
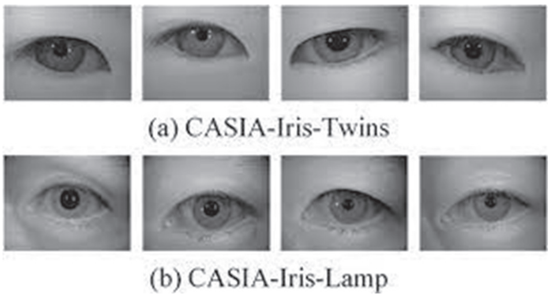

Watermarked Image
2-Level Multiband DTDWT Wavelet Transforms
Select LL₃ Sub-Band
Apply SVD on A*, A* = U*S*V*T
Obtain D* = UwS*VwT
Obtain Embedded Watermark as-W*= (D* -S)
Change Double Precision Real Number to Unsigned 8-Bit Integer

Fig. 4. Watermark Extraction Model

4. EXPERIMENTAL RESULTS

In unconditioned cases, the functionality of recognition schemes based on iris images would not produce accurate results. The availability of exactly collected iris image datasets with sufficient measurements will decide the outcome of the research involving the specified complication. Since knowledge is minimal, iris-based identification system analysis and investigation can be done by using the CASIA Iris Image Database sample is shown in Fig. 5.


(a) CASIA-Iris-Twins

(b) CASIA-Iris-Lamp

Fig 5. Sample CASIA Iris Image Database

A. Statistics and Descriptions of the Database

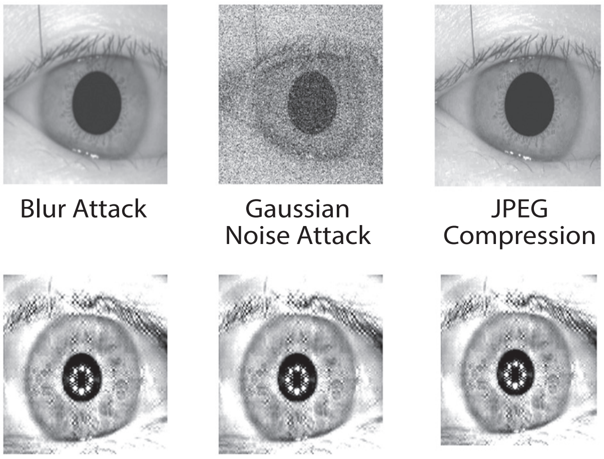
CASIA-IrisV3 has three following subdivisions: CASIA-Iris-Interval, CASIA-Iris-Lamp, and CASIA-Iris-Twins. CASIA-IrisV3 will contain large number of iris images: 22,035 iris images from 700 subjects. The entire set of images will be captured as an 8-bit monochromatic JPEG with near-infrared lighting.

B. Performance Analysis

CASIA iris images are used for iris recognition experiments. Each iris illustration is included with ten iris images taken at various times; the first copy will be used to implant the watermark, while the outstanding nine images will be used for identification. Table 1 shows the results of the recognition experiment.

Figure 6 shows the obtained images and extracted watermark after the attacks. The result will be accessed with the metric such as Correct Recognition Rate (CRR), False Accept Rejection Rate (FAR) and False Rejection Rate (FRR).

The results depicts that the iris biometric data is protected from the being theft by the anonymous users.



Blur Attack

Gaussian Noise Attack

JPEG Compression

Obtained Images after the Attack

Fig 6. Obtained Result Images

Table 1. Biometric Authentication using Iris

Algorithm/Attacks	**Proposed Multiband DTDWT**			**DWT based Watermarking**		
Nature of Attacks	**CRR**	**FAR**	**FRR**	CRR	FAR	FRR
No Attack	**99.4%**	**0.0014**	**0.124**	99.4%	0.0014	0.124
Jpeg Compression Q=70%	**97.3%**	**0.0007**	**0.0041**	96.3%	0.0009	0.0049
Gaussian filtering with Var=3	**98.3%**	**0.0025**	**0.0725**	97.1%	0.0021	0.09
Median Filtering (3x3)	**97.3%**	**0.0041**	**0.034**	96.5%	0.0040	0.03
Blurring	**97.1%**	**0.0030**	**0.0281**	96.9%	0.0045	0.0881

For evaluating the functionality of suggested biometric watermarking approaches in the context of the following scenarios: Jpeg Compression kept at 70% quality, Gaussian filtering with variance kept as 3pixel, median filtering in 3x3 Window and blurring with (3*3) Mask. The proposed Multiband DTDWT rate is higher than the existing DWT based Watermarking using Iris Biometric Authentication System.

5. CONCLUSION

Multi-band DTDWT watermarks can withstand frequency attacks, while DWT-based watermarks can resist regular attacks. This article proposes a new biometric image watermarking procedure that syndicate Multi-band DTDWT and SVD-based algorithms that can increase durability and resilience when exposed to geometric and frequency attacks. The biometric recognition procedure is used as an index, comprehensive recital of the iris biometric watermark. The experimental outcomes show that the watermark procedure is more robust against geometric and frequency attacks compared to DWT-based watermarking. This algorithm can also preserve the integrity of the iris biometric template. Finally, the proposed framework can be applied not only to the assessment of iris biometrics, but also to other areas where privacy is critical. For example, user profiles on social media can provide benefits such as content or travel advice, but also recover sensitive information from seemingly anonymous data.

The proposed Multiband discrete wavelet transform and singular value decomposition technique enhances the security of the iris biometric system than the existing authentication techniques.

- We embed watermark in the principle components of the multi-band discrete wavelet coefficients. Specifically, the watermark signal is embedded into the principle components of the multi-band wavelet coefficients corresponding to the same spatial location at the same scale. With such a well-chosen embedding domain, the watermark is robustly and efficiently distributed to every detail frequency sub band. Our experimental results have shown that the watermark thus embedded has better invisibility and is more robust against JPEG compression than watermarks embedded in the DWT domain.
- Parameterized multi-band wavelet leads to a more secure watermark embedding domain, which makes the attack more difficult.
- Different from many other watermarking schemes,

in which watermark detection threshold is chosen empirically, the detection threshold of the proposed watermarking scheme can be calculated according to the targeted false positive.

6. REFERENCES

[1]. S. Katzenbeisser, F. A. P. Petitcolas, "Information hiding techniques for steganography and digital watermarking", Artech house, Computer security series, 2000.

[2]. N. F. Johnson, Z. Duric, S. Jajodia, "Information hiding, steganography", Kluwer Academic Publisher, 2003, pp. 15-29.

[3]. S. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 11, 1989, pp. 674-693.

[4]. X. Zhu, J. Zhao, H. Xu, "A digital watermarking algorithm and implementation based on improved SVD watermarking-attacks and counter measures", Proceedings of the 18th IEEE Conference on Computer Vision and Pattern Recognition.

[5]. Iris recognition, https://en.wikipedia.org/wiki/Iris_recognition#Advantages (accessed: 2022)

[6]. T. Hoang, D. Tran, D. Sharma, "Bit priority based biometric watermarking", Proceedings of the Second International Conference on Communications and Electronics, Hoi An, Vietnam, 4-6 June 2008, pp. 191-195.

[7]. Technavio, https://www.techavio.com/report/iris-recognition-market-industry-analysis (accessed: 2022)

[8]. J. Dong, T. Tan, "Effects of watermarking on iris recognition performance", Proceedings of the 10th International Conference on Control, Automation, Robotics and Vision, Hanoi, Vietnam, 17-20 December 2008.

[9]. S. Majumder, T. S. Dutta, "Watermarking of data using biometrics", Handbook of research on computational intelligence for engineering, science and business, IGI Global, 2020, p. 623.

[10]. Q. Zhao, "Advanced information security technology: watermarking and biometrics", ACM-HK Student Research and Day, 2009.

[11]. G. Varbanov, P. Blagoev, "An improving model watermarking with iris biometric code", Proceedings of the International conference on Computer systems and technologies, June 2007.

[12]. D. P. Mukherjee, S. Maitra, S. T. Acton, "Spatial domain digital watermarking of multimedia objects for buyer authentication", IEEE Transactions on Multimedia, Vol. 6, No. 1, 2004, pp. 1-15.

[13]. A. K. Singh, N. Sharma, M. Dave, A. Mohan, "A novel technique for digital image watermarking in spatial domain", Proceedings of the 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, India, 6-8 December 2012, pp. 497-501.

[14]. Y. Wang, J. F. Doherty, R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Transactions on Image Processing, Vol. 11, No. 2, 2002, pp. 77-88.

[15]. W. Wang, A. Men, X. Chen, "Robust image watermarking scheme based on phase features in DFT domain and generalized radon transformations", Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, 17-19 October 2009, pp. 1-5.

[16]. M. N. Sakib, S. B. Alam, A. B. M. R. Sazzad, C. Shahnaz, S. A. Fattah, "A basic digital watermarking algorithm in discrete cosine transformation domain", Proceedings of the Second International Conference on Intelligent Systems, Modelling and Simulation, Phnom Penh, Cambodia, 25-27 January 2011, pp. 419- 421.

[17]. K. Deb, M. S. Al-Seraj, M. M. Hoque, M. I. H. Sarkar, "Combined DWT-DCT based digital image watermarking technique for copyright protection", Proceedings of the 7th International Conference on Electrical and Computer Engineering, Dhaka, Bangladesh, 20-22 December 2012, pp. 458-461.

[18]. P. Dabas, K. Khanna, "A study on spatial and transform domain watermarking techniques", International Journal of Computer Applications, Vol. 71, No. 14, 2013, pp. 38-41.

[19]. A. K. Jain, U. Uludag, "Hiding biometric data", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 25, No. 11, 2003, pp. 1494-1498.

[20]. M. Vatsa, R. Singh, A. Noore, "Improving biometric recognition accuracy and robustness using DWT and SVM watermarking", IEICE Electronics Express, Vol. 2, No. 12, 2005, pp. 362-367.

[21]. C. Y. Low, A. B. J. Teoh, C. Tee, "A preliminary study on biometric watermarking for offline handwritten signature", Proceedings of the IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Penang, Malaysia, 14-17 May 2007, pp. 691-696.

[22]. M. Fouad, A. El Saddik, Z. Jiying, E. Petriu, "Combining cryptography and watermarking to secure revocable iris templates", Proceedings of the IEEE International Instrumentation and Measurement Technology Conference, Hangzhou, China, May 2011, pp. 1-4.

[23]. S. Majumder, K. J. Devi, S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking", IET Biometrics, Vol. 2, No. 1, 2013, pp. 21-27.

[24]. M. Paunwala, S. Patnaik, "Biometric template protection with DCT- based watermarking", Machine Vision and Applications, Vol. 25, No. 1, 2014, pp. 263-275.

[25]. J. Lu, T. Qu, H. R. Karimi, "Novel iris biometric watermarking based on singular value decomposition and discrete cosine transform", Mathematical Problems in Engineering, Vol. 2014, 2014, pp. 1-6.