A Robust Approach for Security and Integrity of Biometric Images Using Wavelet-SVD Operation

Madhuri Yadav, Ankita Dwivedi and Mohit

October 3, 2022

A Robust Approach for Security and Integrity of Biometric Images using Wavelet-SVD Operation

Madhuri Yadav[1], Ankita Dwivedi[1], Mohit[1]
[1]Department of Computer Science and Engineering, Centre for Advanced Studies, AKTU, Lucknow, India
[1]madhuri.yd@gmail.com , [1]ankitadwivedikit007@gmail.com , [1]mohitsinghrajput73@gmail.com

***Abstract*—Biometric includes images such as fingerprints, iris scans, palm prints, face scan which have fine features of uniqueness for each individual. As these images are serviceable in many applications such as access control, military, CBI investigation, identification, etc., their security is a major concern. An approach for securing biometric images can be Digital Watermarking. Conventional watermarking may distort the image which causes loss of information. Even a small distortion may leave an individual biometric unrecognizable. So there is a crucial need of a watermarking scheme which does not distort the host image at all. This paper introduces a zero watermarking scheme in which unique identification codes are generated from biometric images by applying Discrete Wavelet Transform (DWT) followed by Singular Value Decomposition (SVD). Experimental results illustrate that unique features extracted are highly stable against multiple image processing attacks and hence promulgate its worth for confidential biometric images.**

Keywords—Biometric Images, BER, DWT-SVD, Image processing attacks, NC, Robust, Zero bit watermarking.

I. INTRODUCTION

Biometric features are a metric of human characteristics which is used for identification, authentication and confidentiality in an assortment of applications. The human identification by the physical feature is measured and checked. The authentication also provides secure and reliable method to prevent from growing identity theft for the secured database. But human characteristics are not even safer nowadays which leads to loss of the confidential data [1].

Various applications of authentication using biometric features are access control of nuclear power plant, computers in military to secure the borders, in CBI for identifying the criminals, issuing identify proofs, passports, in forensic labs to secure the medical database, security in airport, etc. [2]. A password or a key for the access of protected data is biometric image like face scan iris, palm print, fingerprint, etc. Security of such systems which uses different types of biometric for making the unique identity of individuals is very important. The face recognition is the most matured technology and used for authentication in several applications like mobile phones, google photos, issuing identity documents, face checks at border to analyze digital biometric passport with individual's face and hence intricate for masquerader to get the access. Some methods of attacks are by direct hacking the database or hoax the face scan stored information [3]. Some of the threats to biometric systems are spoofing, DOS (Denial of service), collusion and coercion, also the evasion and refusal.

Biometric images can be attacked by any uncertified person who imposes the fake biometric to biometric sensor and then hack the system. Trojan horse program put in the place of actual software program in the device can extract and match the face scan. Hence to prevent the database of face scan information, the watermarking technique is a way towards the face scan data security [4].

The watermark embedding will lead to distortion in the face scan data and the extraction creates the unguarded situations as the watermark removed from the face scan image will be at danger under these circumstances [5].

The key contribution of the paper is watermarking scheme using a zero bit technique that does not at all tamper the host biometric images and hence is able to get the original print without altering the final image. Unlike conventional watermarking, it does not embed the watermark or the data into the host image. Hence the information loss does not take place. Quality and reliability of the host image is well maintained. As unique features extracted are highly robust against various image processing attacks, consequently, the given methodology is also robust to several attacks of image processing like contrast enhancement, Gaussian and median filtering, histogram equalization, JPEG compression. Proposed algorithm is a one of the possible ways out to provide security for Biometric systems [6].

Organization of rest of the paper is as follows. Section II discusses the techniques used during embedding and extraction of watermark. Section III states the proposed algorithms. Section IV describes the experimental results which show the correctness of algorithm by comparing the correlation coefficients and lastly, Section V gives the conclusion of the paper and some of the future work.

II. PRELIMINARIES

This section defines the basics required for understanding the proposed watermarking scheme.

A. Singular Value Decomposition (SVD)

Singular Value Decomposition decomposes a matrix and useful in watermarking techniques because little deviation in the singular values do not influence image's quality as they are very much stable in nature, they do not alter even after application of several attacks of image processing [7]. The method of getting singular values is as follows:

Let's consider a matrix P with dimension x*y on which SVD is applied. It generates a matrix D which is a diagonal matrix and consists of positive diagonal elements i.e., $\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_\rho$ that are in decreasing order and has same dimensions as P and the rank of P is ρ. Two another matrices, U and V are obtained which are unitary orthogonal matrices having u_k and v_k column vectors respectively [8].

$$P=UDV^T=(u1, u2, u3, \ldots, un)\begin{bmatrix}\Sigma & 0\\ 0 & 0\end{bmatrix}(v1, v2, v3, \ldots, vn)^T \quad (1)$$

$$\Sigma = \text{diagonal}\ (\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_\rho) \quad (2)$$

Where,

$$\sigma_1 \geq \sigma_2 \geq \sigma_3 \geq \cdots \sigma_\rho \geq \sigma_{\rho+1}, \sigma_{\rho+2} = \cdots = \sigma_n = 0$$

B. *Discrete Wavelet Transform*

The multi-regional disintegration of images is done by an indispensable procedure called Discrete Wavelet Transform (DWT). This transformation can be performed in multiple stages. In the beginning, an image is disintegrated into following sub-bands that are LL1, HL1, LH1, and HH1, where the finest(detailed image) scale wavelet coefficients are obtained by HL1, LH1 and HH1 sub-bands, whereas coarse level (approximation image) coefficients are obtained byLL1 sub-band. Now, in order to achieve further level of wavelet coefficients, the LL1 sub-band is again disintegrate into four sub bands LL2, HL2, LH2, and HH2 and this disintegration process of multiple regions or resolution of image can be continued until a particular last stage is arrived depending on the application of user [9]. The wavelet disintegration of an image in two levels is shown in figure 1.

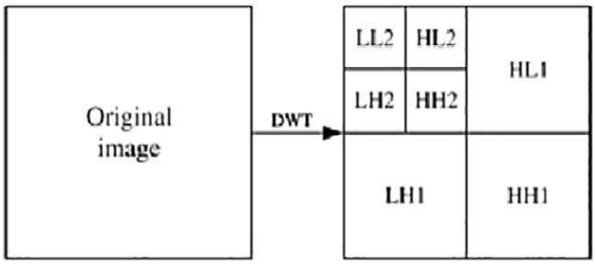


Fig. 1. Discrete Wavelet Transformation of two levels

Wavelet is one of the promising domains for watermark embedding because in time and spatial domain both, it allows good localization. For the purpose of embedding, the regions which give the facility to increase the watermark's robustness are selected. DWT offers ample information and requires lesser time of computation for examining host signal. The Haar wavelet has been used for the disintegration process as its transform has many advantages which are as following: i) fast, ii) memory competent iii) abstractly easy, and iv) in other wavelet transforms, the edge effects is an issue but haar is accurately reversible without these edge effects[10].

III. Proposed Scheme

The proposed method is based upon distinctive characteristics extraction from the biometric images that is done by applying Discrete Wavelet Transform (DWT) to convert the biometric image and then non concurring blocks of magnitude n*n are made by splitting the LL approximation sub-band. There is a minimum change in pixel value of LL approximation sub-band than the LH, HL, HH detailed sub-bands, on applying the image processing attacks. And then, singular values are found by SVD of each block, which is always unique and therefore it's contributing in unique feature generation and extraction. A distinctive logical matrix is generated using every block's singular values, and this distinctive characteristic is then tactically integrated with the ID of individual to create master share [11]. Figure 2 shows one of the sample host image of face scan database, watermark and corresponding master share in the experiment.

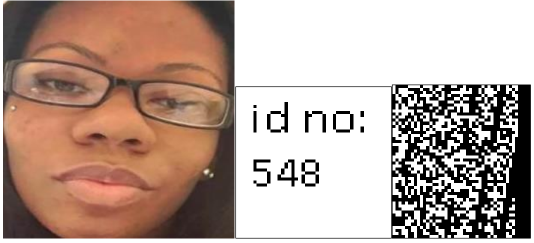


Fig. 2. Host image, watermark, secret key

The process of embedding is explained in the following steps:

A. *Algorithm 1: Embedding Process*

(1) The multiple face scan images from the directory will be read and on each of the image DWT is performed to disintegrate them into LL, HL, LH and HH sub-bands.

$$\text{DWT (I)} = [\text{LL}, \text{HL}, \text{LH}, \text{HH}]$$

(2) Consider the sub-band i.e., LL and divide it into blocks, B_k that should be non-concurrent and of magnitude n*n. Here, k=1, 2, 3…, N and N is the total blocks used for the embedding watermark and its size must be equal to watermark (i.e., number of bits in watermark). Dimension of block has been taken as 4*4 for the experimental purpose.

(3) SVD is applied to every block B_k of every image.

$$\text{SVD } (B_k) = [U_k, D_k, V_k] \quad \text{where,}$$
$$Dk = \text{diagonal}\ (\sigma k1, \sigma k2, \sigma k3, \ldots, \sigma kq, 0, \ldots 0)$$

(4) A 'temporary' matrix will be declared which stores the initial singular value D_k (σ_{k1}) of every block B_k, i.e.,

$$\text{temporary (k)} = D_k\ (\sigma_{k1})$$

(5) Consider the two successive values of 'temporary' in a row say, a and b, then following operation performed:

If a>=b *Then bit=1;*
Else if a<b *Then bit=0;*

The generated bit stored in a matrix 'G' every time, where the matrix G(logical) generated is of same size as 'temporary' for every image.

(6) Take the binary watermark image and then execute encryption (Arnold Scrambling).

(7) The encrypted watermark image and the matrix G are obtained from above steps. Perform the XOR(logical) operation on both i.e.,

$$z = \text{XOR (G, watermark)}$$

(8) Execute Arnold Cat Map encryption on z which gives the secret key K' (also called master share) is send to receiver and watermark/ID will be extracted.

$$K' = \text{encryption (z)}$$

Extraction process includes extraction of distinctive characteristics same as in embedding procedure. To fetch the original person's ID or details, distinctive characteristics are critically merged with resulting master share. The process of extraction is explained stepwise as follows:

B. *Algorithm 2: Extraction Process*

(1) The multiple face scan images from the directory will be read and in each of the image, DWT is performed to disintegrate them into LL, HL, LH and HH sub-bands.

$$\mathrm{DWT}\ (\mathrm{I})\ =\ [\mathrm{LL}, \mathrm{HL}, \mathrm{LH}, \mathrm{HH}]$$

(2) Consider the sub-band i.e., LLand divide it into blocks, B_k that should be non-concurrent and of magnitude n*n. Here, k=1, 2, 3…, N and N is the total blocks used for the embedding watermark and its size must be equal to watermark (i.e., number of bits in watermark). Dimension of block taken as 4*4 for the experimental purpose.

(3) SVD is applied to each block B_k of every image.

$$\mathrm{SVD}\ (B_k) = [U_k, D_k, V_k] \quad \text{where,}$$

$$Dk = \text{diagonal}\ (\sigma k1, \sigma k2, \sigma k3, \dots, \sigma kq, 0, \dots 0)$$

(4) A ‘temporary’ matrix will be declared which stores the initial singular value D_k (σ_{k1}) of every block B_k, i.e.,

$$\text{temporary (k)} = D_k\ (\sigma_{k1})$$

(5) Consider the two successive values of ‘temporary’ in a row say, a and b then following operation performed:

If a>=b *Then bit=1;*
Else if a<b *Then bit=0;*

The generated bit stored in a matrix ‘G’ every time, where the matrix G (logical) generated is of same size as ‘temporary’ of every image.

(6) On the master share K’ of every image perform lossless decryption by Arnold Cat Map.

$$z = \text{decryption (K')}$$

(7) Execute the XOR (logical) operation on z and G to extract watermark/ original person’s identity.

$$\text{Watermark} = \text{XOR (G, z)}$$

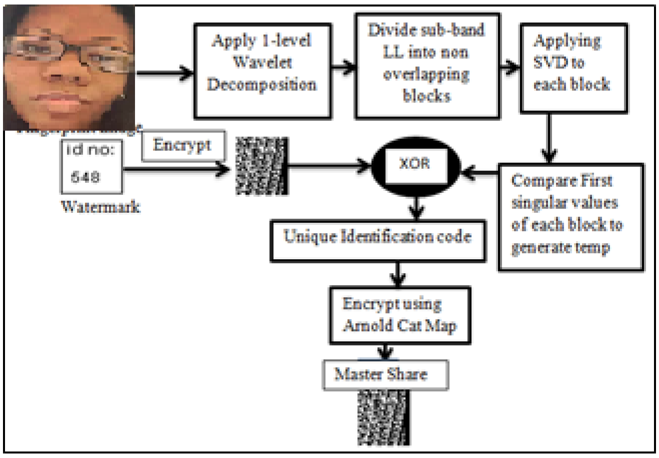

Apply 1-level Wavelet Decomposition
Divide sub-band LL into non overlapping blocks
Applying SVD to each block
id no: 548
Watermark
Encrypt
XOR
Compare First singular values of each block to generate temp
Unique Identification code
Encrypt using Arnold Cat Map
Master Share

Fig. 3. Embedding Process of multiple images using zero bit watermarking

Figure 3 shows embedding process by proposed algorithm in which DWT is used followed by SVD, the first singular values of each block of biometric image is XOR with the encrypted watermark and gives unique identification code.

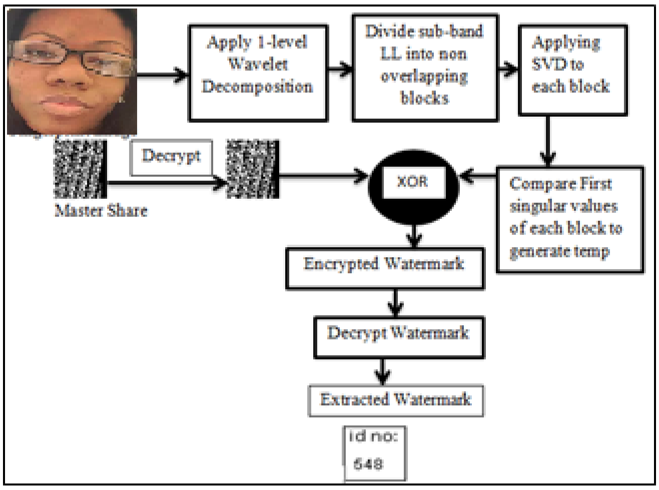

Apply 1-level Wavelet Decomposition
Divide sub-band LL into non overlapping blocks
Applying SVD to each block
Decrypt
Master Share
XOR
Compare First singular values of each block to generate temp
Encrypted Watermark
Decrypt Watermark
Extracted Watermark
id no: 548

Fig. 4. Extraction process of multiple images using zero bit watermarking

Figure 4 shows extraction process by proposed algorithm in which using DWT and SVD the first singular values of each block of biometric image is XOR with the decrypted unique code (master share) and gives the extracted watermark which is the individual’s ID.

IV. Experimental Results

This segment elaborates the experimental outcomes of proposed algorithm. It was implemented on 50 biometric images of the standard database of kaggle gender detection face (https://www.kaggle.com/gmlmrinalini/genderdetectionface) whose aftermath are shown in this segment. Figure 5 shows three original images, original person’s ID information, corresponding master shares generated by the proposed algorithm and the extracted biometric id. Quantitative analysis was accomplished to examine the proposed algorithm.

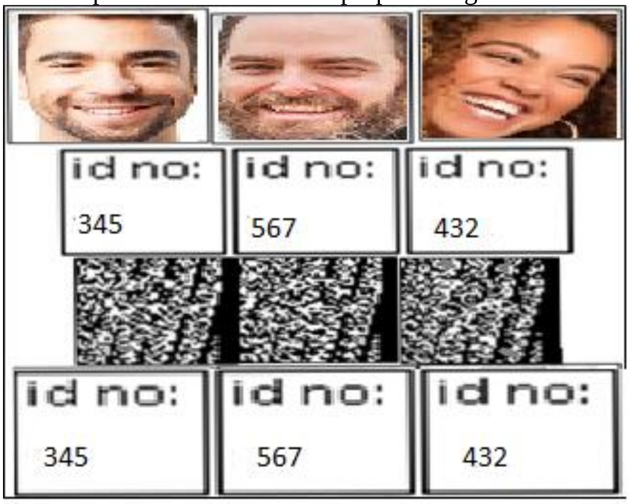
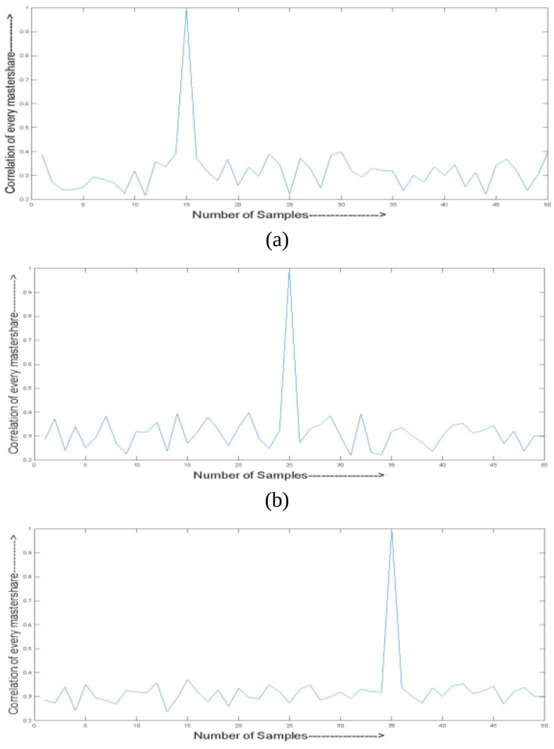


Fig. 5. Original images with corresponding watermarks and its master share generated by embedding process then the id obtained by extraction process.

C. *Correlation coefficient*

It is a numeric value of relation between two variables. Here, the variables are master share of different host images. The maximum value of Correlation coefficient is 1 that denotes that master shares are thoroughly identical and the minimum value of Correlation coefficient is 0 that denotes that master share are absolutely divergent i.e., the algorithm is working properly and all the master share are unique [12].

To validate the embedding and extraction process, master share of each image is compared with one of the master share i.e., the sample compared with 15th, 25th and 35th sample of biometric image in terms of the correlation coefficient in Figure (a), (b), (c) respectively.



(a)

(b)

(c)

Fig. 6. Graph of correlation coefficients defines the uniqueness of master share or key and correctness of algorithm (a)Uniqueness for 15th sample (b) for 25th sample (c) For35th sample.

From the distinguished values of correlation in Fig. 6 between every master share we can infer that all the master shares are unique from each other and hence image is properly encrypted, identified uniquely by their master share on receiver side and extracted to give the individual's ID. And this proves the correctness of proposed algorithm.

D. Normalized Correlation (NC)

The similarity component between two data is Normalized Correlation. This can be analyzed as below. Let the original watermark be I and extract watermark is I", both are of same dimension i.e., m*n. Then the normalized correlation is given as [13]:

$$\text{NC (I, I*)} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} I(i,j).I*(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n} I(i,j)^2} \qquad (3)$$

E. Bit Error Rate (BER)

BER is the proportion between numerals of miscalculation in bits and overall numerals of bits of the watermark. Let W be real image and W" be attacked image both are of same magnitude i.e., m*n. Then the bit rate error is calculated as [14]:

$$\text{BER (W, W*)} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)\oplus W*(i,j)}{m*n} \qquad (4)$$

where, ⊕ is the XOR operation, i is row and j is column variable.

Table I shows the result of NC and BER between indigenous and extracted watermark of 40 sample face scan images, without any attacks.

TABLE I. Value of NC and BER without attacks

Biometric Images	Normalized Correlation	Bit Error Rate	Biometric Images	Normalized Correlation	Bit Error Rate
1	1	0	21	1	0
2	1	0	22	1	0
3	1	0	23	1	0
4	1	0	24	1	0
5	1	0	25	1	0
6	1	0	26	1	0
7	1	0	27	1	0
8	1	0	28	1	0
9	1	0	29	1	0
10	1	0	30	1	0
11	1	0	31	1	0
12	1	0	32	1	0
13	1	0	33	1	0
14	1	0	34	1	0
15	1	0	35	1	0
16	1	0	36	1	0
17	1	0	37	1	0
18	1	0	38	1	0
19	1	0	39	1	0
20	1	0	40	1	0

The values of NC and BER in table I are 1 and 0 respectively, which depicts that after extraction, watermark is reconstructed in exactly same form as inserted during embedding. Hence when no attacks are applied the data loss is zero and the individual's ID is perfectly recovered on receiver side.

Now, whenever attacks are applied to the original image, unique features, which is being extracted to generate master share, will get distorted, therefore, leading to distorted watermark extraction. The more robust/stable are the unique features, more robust will be the watermark extraction from master share. Singular values have been used for unique feature generation because they are very stable in nature. Attacks on image do not change singular values considerably.

Any watermark algorithm is stable/robust when identifiable watermark can be recovered and that happens when value of NC is greater than 0.8 of indigenous and attacked image. Another parameter for calculating the robustness is BER.

Table II represents average NC and BER of 40 samples between original and attacked watermark using proposed algorithm.

TABLE II. Average value of NC and BER with attacks

Attacks	Normalized correlation	Bit Error Rate
No attack	1	0
JPEG Compression	0.9899	0.0179
Median Filter	0.9685	0.0276
Gaussian Filter	0.9795	0.0706
Sharpening	0.9593	0.0128
Histogram Equalization	0.9318	0.0293

Contrast Enhancement	0.8567	0.0134
Blurring	0.6918	0.0837

From the above table, it is clearly confirmed that the robustness of algorithm as in most of the samples, NC values is more than 0.85, also the value of BER approaches to zero against JPEG compression, median filtering, Gaussian filtering, sharpening, histogram equalization, contrast enhancement attacks and moderately robust against blurring attack and therefore clearly achieving the purpose [15][16].

The performance of proposed algorithm can be also determined by the computational time required to execute the proposed algorithm. Table III displays the computation time of 40 samples implementing the zero-bit watermarking.

TABLE III. Computational time of execution of algorithm.

Biometric Images	Computational Time (in seconds)	Biometric Images	Computational Time (in seconds)
1	2.856	21	2.231
2	2.867	22	2.567
3	2.989	23	2.943
4	2.567	24	2.654
5	2.962	25	2.897
6	2.966	26	2.951
7	2.897	27	2.753
8	2.825	28	2.736
9	2.765	29	2.097
10	2.087	30	2.876
11	2.981	31	2.432
12	2.765	32	2.234
13	2.980	33	2.674
14	2.896	34	2.032
15	2.574	35	2.543
16	2.879	36	2.967
17	2.854	37	2.897
18	2.876	38	2.685
19	2.865	39	2.978
20	2.982	40	2.564

Hence, the above table III demonstrates that proposed algorithm is useful in real time applications of biometric images.

V. Conclusion And Future Work

The zero-bit watermarking technique enables to embed the watermark without distorting the host image. In biometric images, least distortion can change the individual unique identity, hence proposed work is preferred for application in biometric images. SVD and DWT are used to generate unique features in the proposed algorithm which is thoroughly tested and the experimental results signify that the embedding of watermark is properly accomplished as the master share of every host image is unique. Also, proposed algorithm is robust to the several image processing attacks as is evident through the experimental results. It can be concluded that the proposed work is a practical way to secure the biometric images for security applications like crime investigation, attendance and authentication, etc.

VI. References

[1] Mehta, Garima, Malay Kishore Dutta, RadimBurget, and Vaclav Uher. "Edge based block wise selective fingerprint image encryption usingchaos", 2015 38th International Conference on Telecommunications and Signal Processing (TSP), 2015.

[2] Chunlei Li, Yunhong Wang, Bin Ma, Zhaoxiang Zhang, Tamper detection and self-recovery of biometric images using salient region based authentication watermarking scheme, Computer Standards & Interfaces, Volume 34, Issue 4, 2012, Pages 367-379, ISSN 0920-5489

[3] Dutta MK, Singh A, Soni KM, Burget R, Riha K (2013) Watermark generation from fingerprint features for digital right management control. 36th IEEE International Conference on Telecommunications and Signal Processing, Rome, Italy 717–721.

[4] Thanki R., Borisagar K. (2016) Biometric Watermarking Technique Based on CS Theory and Fast Discrete Curvelet Transform for Face and Fingerprint Protection. In: Thampi S., Bandyopadhyay S., Krishnan S., Li KC., Mosin S., Ma M. (eds) Advances in Signal Processing and Intelligent Recognition Systems. Advances in Intelligent Systems and Computing, vol 425. Springer, Cham.

[5] Abhilasha Singh, Malay Kishore Dutta. "A robust zero-watermarking scheme for tele-ophthalmological applications", Journal of King Saud University - Computer and Information Sciences, 2017

[6] Feng Wen-ge, Liu Lei. "SVD and DWT zero-bit watermarking algorithm", 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR 2010),2010

[7] Yaxun Zhou, and Wei Jin. "A novel image zero watermarking scheme based on DWT SVD", 2011 International Conference on Multimedia Technology, 2011.

[8] Chunhua Dong, Jing bing Li, Yen-wei Chen, Yong Bai, "Zero watermarking for medical images based on DFT and LFSR," 2012 IEEE International Conference on in Computer Science and Automation Engineering (CSAE), , vol.1, pp.22-26, May 2012.

[9] V. Seenivasagam and R. Velumani "A QR Code Based Zero Watermarking Scheme for Authentication of Medical Images in Teleradiology Cloud" Computational and Mathematical Methods in Medicine, Hindawi Publishing Corporation, 2013, Article ID 516465.

[10] C. Dong, H. Zhang, J. Li, and Y. W. Chen, "Robust zero watermarking for medical image based on DCT," in Proceedings of IEEE 6th International Conference on Computer Sciences and Convergence Information Technology, pp. 900–904, 2011.

[11] Xiaonian Tang; Jianchun Wang; Chengbao Zhang; Huiming Zhu; YanFu, "A fast and low complexity zero-watermarking based on average sub image in multiwavelet domain," 2nd International Conference onin Future Computer and Communication (ICFCC), vol.2, no., pp.178-182, May 2010.

[12] Park K.R., Jeong D.S., Kang B.J., Lee E.C. (2007) A Study on Iris Feature Watermarking on Face Data. In: Beliczynski B., Dzielinski A., Iwanowski M., Ribeiro B. (eds) Adaptive and Natural Computing Algorithms. ICANNGA 2007. Lecture Notes in Computer Science, vol 4432. Springer, Berlin, Heidelberg.

[13] Hung-Hsu Tsaia, Yen-Shou Lai, Shih-Che Lob, "A zero-watermark scheme with geometrical invariants using SVM and PSO against geometrical attacks for image protection" The Journal of Systems and Software, Elsevier, 86 (2013) pp. 335– 348.

[14] Ankita Dwivedi, Ankit Kumar, Malay Kishore Dutta, Radim Burget, Vojtech Myska. "An Efficient and Robust Zero-Bit Watermarking Technique for Biometric Image Protection", 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), 2019.

[15] A. Singh, N. Raghuvanshi, M. K. Dutta, R. Burget and J. Masek, "An SVD based zero watermarking scheme for authentication of medical images for tele-medicine applications," 2016 39th International Conference on Telecommunications and Signal Processing (TSP), Vienna, 2016, pp. 511-514.

[16] Garima Mehta, Malay Kishore Dutta, Jan Karasek&Pyung Soo Kim, "An Efficient and Lossless Fingerprint Encryption Algorithm using Henon Map and Arnold Transformation" - IEEE International Conference on Control, Communication and Computing, December 2013, pp.1-6, Proceedings published by IEEE Xplore, New York, USA.